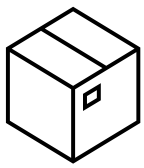
Counter Fraud Newsletter – January 2023

Happy New Year and welcome to the January edition of the Audit Yorkshire Counter Fraud Newsletter for NHS staff.

Current Scam Trends

Supplier scams
It may come as a surprise the lengths fraudsters will go to in order to trick you out of your money. Some NHS organisations have recently been targeted by fake suppliers.



The fraudster pretends to be from a company that may well do business with the NHS, such as those selling printer cartridges or PPE. They then create a fake invoice and send it in. Some of these invoices are for very low amounts, and the fraudsters are hoping that no checks will be made.

We have seen this happen before, but the fraudsters are stepping up a gear. Additional tactics we have seen include:

- The fraudsters set up a PO box for mail so they cannot be traced.
- They will scrutinise job vacancies and try to see who will be new in post. This is who they will target in hope that they are not familiar with what has been ordered before they started working there.
- A parcel with few items in it, or even an empty box is posted with the recipient being asked to sign for the delivery. This proof of delivery is then used to claim that as the parcel has been accepted, it must be paid for.
- Threats to add late fees and/or refer to a debt collection agency unless payment is made immediately.

Investment Fraud

Investment fraud is a growing industry for fraudsters – statistics published by the City of London Police recorded a 49.5% increase in investment scams between 2020/2021 and 2021/2022. The average loss to victims was over £34,000.

As the cost of living continues to bite, people may be lured into investment scams as they claim they will quickly produce significant financial gains. You can find some advice below on keeping yourself safe from this type of fraud:

- **Don't be rushed:** Remember, legitimate organisations will never pressure you into investing on the spot.
- **Be wary of false endorsements:** fraudsters hijack social media accounts to make it look like someone you trust (such as a favourite celebrity or a family member) has already invested in the scheme with great success.
- **Seek advice first:** Before making significant financial decisions, speak with trusted friends or family members, or seek professional independent advice.
- **Financial Conduct Authority (FCA) register:** Use the FCA register to check if the company is regulated. If you deal with a firm (or individual) that isn't regulated by the FCA, you may not be covered by the Financial Ombudsman Service (FOS) if things go wrong and you lose your money. For more information about how to invest safely, please visit: https://www.fca.org.uk/scamsmart

What to do if you've been a victim of Financial Investment fraud:

Report it: Inform your bank as soon as possible. They may be able to freeze or recover payments, depending on what has happened. You can also report it to Action Fraud online at actionfraud.police.uk or by calling 0300 123 2040.

Be aware that you could be targeted again: Fraudsters sometimes re-establish contact with previous victims claiming that they can help them recover lost money, this is just a secondary scam. Hang up on any callers making these claims.

Identity theft: If you suspect your identity may have been stolen, you can check your credit rating quickly and easily online. You should do this every few months anyway, using a reputable service provider and follow up on any unexpected or suspicious results.

Legal advice: Seek professional legal advice or contact Citizens Advice https://www.citizensadvice.org.uk/ to understand your options.

You can also contact the Financial Conduct Authority's, www.fca.org.uk, consumer helpline on 0800 111 6768 or report suspicious businesses or individuals by using the reporting form on their website.

New Year, New Password

When was the last time you changed the password on your personal email account? At work, we all get prompted to reset our password once a year. But, many of us will cling to the same password for our personal email account for many years.

The start of a new year can be a good prompt to update your email password and review your other security settings.

Your email account is particularly attractive to fraudsters. If they manage to take it over, they can go around common retailers and services where your details may be stored - such as Amazon, PayPal, Facebook, Instagram, and eBay. They can enter your email address and request a password reset for these other accounts.

Most password resets involve an email being sent containing a password reset link. This gives fraudsters the ability to reset your passwords and effectively lock you out of important accounts. These accounts may contain your payment details, home address, and other sensitive information to make it easy to quickly order items/send money.

On top of that, the fraudster could use your personal email account to target your friends and family with phishing emails designed to look like they have come from you.

The National Cyber Security Centre advise that if you have used your email password anywhere else, you should update it as soon as possible. You should use a strong password which is different to all of your other accounts.

Ideally, all of your accounts should have their own unique passwords. Where it is available, you should also make sure to activate multi-factor authentication. This allows you to add an extra step into your log in process – such as entering a one-time code which is sent to you via text, using a biometric scanner, or authorising the log in attempt on an authenticator app.

Although it may seem like a faff having an additional step to take, having multi-factor authentication active can offer good protection to your account. Even if a fraudster manages to guess or steal your password, they won't be able to get in without providing the second piece of evidence that they are you!

Setting a good password

When picking a password, you should aim for something that someone who knows you wouldn't be able to guess within 20 attempts. That means staying away from the names of loved ones, pets, favourite sports teams, musicians, dates of birth, holiday destinations, and common passwords such as qwerty, password, and 123456 (for more on the most popular passwords, read this BBC article).

People seem to quite like adding numbers into our passwords instead of letters (e.g. P455W0RD) – but cyber criminals are very aware of this tactic too.

Advice from the National Cyber Security Centre (NCSC) is to use three random words. The traditional advice is to make passwords as complex as possible, but that also makes them much harder for us to remember and we then tend to stick to one password once we've learnt it. The NCSC logic is that by putting three unconnected words together, we make passwords that are much harder to guess but pretty easy for us to remember.

If you want to read more about why the NCSC recommend the use of three random words, and their other advice around password management, please see this blog post on their website. The article also explains why the NCSC don't mind you writing your passwords down, as long as you store them safely.

If you can create a mental image around your three random words, this can help you to remember it more easily.

Example 1 – a traditional "complex" password featuring capital letters, numbers and symbols:

Um8r311@ - this password would be cracked by a computer in roughly 8 hours*

Example 2 – three random words:

caravanteapotmouse – this password would be cracked by a computer in around 23 million years*

*Figures calculated by the password checker at www.security.org/how-secure-is-my-password/

In the Press

NHS Pharmacist Suspended for £3.5k Fraud

Abbas Samnani has been suspended for 9 months by a Pharmacy Regulation Tribunal panel, which heard that he had provided false information on his timesheets 30 times in a 39 week period. This led to him overclaiming £3,440.30 from the NHS for 65 hours which he had not worked.

Samnani was caught out when his colleagues at St Mary's Hospital on the Isle of Wight became suspicious. They had been unable to find him when he was needed for "urgent" work. On one occasion he had left work at 09:30 but claimed on his timesheet to have been working until 13:00. Samnani admitted that on the dates in question, that rather than being at work he had been either on the ferry crossing back to the mainland or on his way to the ferry terminal. The tribunal determined that his actions were "serious" and involved "repeated dishonesty". He has now repaid the money in full. You can read more about this story on the Isle of Wight County Press website.

Which? Urges People to Watch Out for Five 2023 Banking Scams

Which? has warned the that the rising cost of living will present criminals with opportunities for fraud in 2023. They have published an article exploring five key scams to look out for in the next year. These include:

- Money mule requests
- Card theft and shoulder surfing
- Fake apps targeting bank accounts
- Calls and texts from "your bank"
- Online purchase scams

You can read more about what these scams are and how to keep yourself safe from them on the Which? website.

A Quick Guide to Reporting Fraud Concerns

I have a concern that fraud may be being committed against the NHS

You can **contact the Counter Fraud team** (you'll find our details on your staff intranet or in your organisation's Anti Fraud, Bribery and Corruption Policy).

You can also report your concerns to the **NHS Counter Fraud Authority** via their online reporting tool or hotline. If you making an anonymous report, **please give as much detail as possible** as we won't be able to contact you for more information.

I have received a suspicious email to my NHS.net email address.

Do not click on any links or attachments.

Forward the suspect email **as an attachment** to **spamreports@nhs.net**.

I have received a suspicious text message

Do not click on any links in the text message!
Forward the text message to **7726.**

I have a concern that fraud may be being committed against the general public

These concerns can be reported to **Action Fraud** (0300 123 2040). If someone has been actively defrauded, it may also be appropriate to report to the **police**. If it is suspected that the victim's bank account has been compromised, they will need to **speak to their bank as a matter of urgency**.

I have received a suspicious email to another email account (not NHS.net)

Do not click on any links or attachments.

Forward the email to **report@phishing.gov.uk.** You can use this option for any suspicious emails you receive on email accounts that are not NHS.net accounts.

I have come across something and I'm not sure whether it is fraud-related

You are very welcome to contact the **Counter Fraud team** for advice and support, our details will be on your staff intranet and in your Anti-Fraud Policy.

You can view previous editions of the counter fraud newsletter on the Audit Yorkshire Website by scanning this QR code.