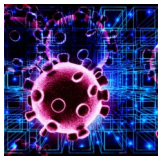
COVID-19 FRAUD ALERTS

ISSUE 2- 06/05/20



Currently the NHS is facing an extremely challenging time due to COVID-19.

We know that during times of crisis some people attempt to take advantage and Audit Yorkshire's aim is to support you through this time by providing fraud advice and guidance.

NHS Related Alerts

Ransomware Risk

Interpol has released a report detailing how some hospitals across the world are being targeted by cybercriminals. There has been an increase in 'ransomware' attacks. This is where a cybercriminal holds information hostage and demands that a ransom is paid before releasing it.

Ransomware is primarily hidden in emails. The recipient may receive an email which appears to be from an official capacity, they are then encouraged to click on a link or attachment which triggers the infection into the organisation's computer system.

The best way to prevent this type of attack is by prevention. Please protect NHS systems by:

- Only opening links and attachments from a trusted source which you are expecting to receive.
- Use a strong password and update it regularly.
- Back up essential information.

Procurement Fraud

You may be aware that NHS England/Improvement recently issued guidance to health bodies allowing prepayment of goods and services during the pandemic. The guidance stipulates that the option can only be exercised in extremely limited and exception circumstances. The guidance can be accessed here.

The guidance details a number of expectations and it is imperative that organisation comply with all of these and fully document their decision-making. From a counter fraud perspective we would discourage organisation from pre-paying for goods and services, however if circumstances leave organisations no other options please feel free to contact your LCFS for advice.

Further advice on protecting your supply chain from fraud during the Covid-19 pandemic has been released by CIPFA. It includes simple and practical advice on fraud pressure points throughout the supply chain, including mandate fraud, due diligence, contract splitting and many others. You can find the guidance here.

Password Advice

The National Cyber Security Centre (NCSC) and the US Department for Homeland Security have issued an advisory notice to all Healthcare Organisations in the UK and USA, due a significant risk of being targeted by "password spraying". This is a technique in which commonly used passwords are tried against known log in information such as email addresses or user names.

The NCSC and the US Department for Homeland Security have advised that all healthcare and medical research staff should reconsider and update their current passwords as appropriate.

They advise that **if you think that your password could reasonably be guessed, you should change it as soon as possible using the "three random words" technique**.

Examples of passwords which are easy to guess include more obvious choices like "password" or "123456", and others which may feel very personal to you but are actually widely used such as "liverpool", "manutd" or "ashley". These passwords all made the list of the most frequently hacked passwords in the UK.

You can use the three random words technique to come up with a password that's still easy for you to remember, but difficult for a criminal to break. Choose three words that have no link between them, and that are not personal to you. For example: **jumpfridgeleaf** is far less likely to be guessed than **onetwothree.** You can further increase the security of your password by adding a number or special character.

You can check the strength of your password at howsecureismypassword.net . Try checking the password examples given above to see how much difference it makes to use random words and adding numbers or characters.

Looking After Yourself Outside of Work

Email Scams

Google have reported that 18 million Covid-19 related hoax emails are being sent to their email users every day. Of the 100 million daily phishing emails which they have blocked over the last week, a fifth have been in relation to Covid-19.

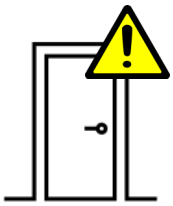
A 'phishing' email is where you are encouraged to reveal personal information, or it may contain a link which when clicked will download a virus onto your computer. Many of these emails are pretending to be from official authorities and organisations. Often the fraudster will try and create a sense of urgency – never feel rushed into responding.

If you click on a dodgy link and only realise afterwards, here's what to do –

- If this was done on a work device, contact IT immediately
- If it is on your own computer, if you have antivirus software, run a full scan. If you don't have antivirus, consider getting it.
- If you have input a password, change your password as a matter of urgency.
- If you have passed on any of your bank details, contact your branch immediately.

You can also forward any suspicious emails to report@phishing.gov.uk. The National Cyber Security Centre's automated programme will test the validity of the site and if found to be a phishing scam, it will be removed immediately.

Door to Door Fraud



There have been many reports throughout North and West Yorkshire in relation to door to door scams. The scams reported so far include –

- Rogue traders trying to sell items such as face masks.
- "Good Samaritans" offering to do shopping for the elderly and vulnerable which ends on them making off with a cash card and pin number.
- People impersonating officials gaining access to homes by saying they are offering COVID-19 testing.

Here's some tips on how to look after yourself and your family.

- Check the ID of any person cold calling. If you make checks with the organisation they are saying they are from, find the number yourself, don't use one which the caller gives you.
- Don't be afraid to ask the person to leave.
- Please make sure that your elderly or vulnerable friends and relatives know that there are dishonest people about who are trying to take advantage

In the news...

Man in court over fake Corona-virus "treatment" kits:

https://www.bbc.co.uk/news/uk-england-london-51991245

UK forces hundreds of scam Covid-19 shops offline:

https://www.bbc.co.uk/news/technology-52361618

Large scale Covid-19 facemask mandate fraud uncovered by Interpol:

https://www.interpol.int/en/News-and-Events/News/2020/Unmasked-International-COVID-19-fraud-exposed

Pharmacist arrested on suspicion of selling home Covid-19 testing kits

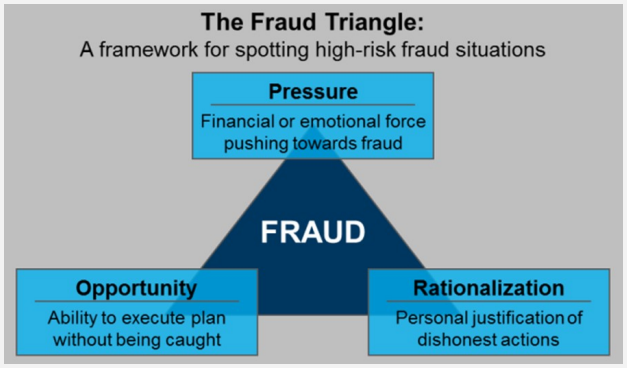
https://www.thepharmacist.co.uk/covid-19/pharmacist-arrested-on-suspicion-of-selling-home-covid-19-testing-kits/

Surveyor arrested for fraud after 250 Covid-19 tests found in his vehicle

https://www.mylondon.news/news/west-london-news/london-coronavirus-uxbridge-surveyor-arrested-18092835

Why are we seeing more fraud at the moment?

There is no doubt that fraud levels have increased since the beginning of the Covid-19 Pandemic. The 'fraud triangle' or 'Cressey's triangle' is a commonly used model to explain why people commit fraud.



There needs to be a **pressure** – a desire to obtain additional funds whether through greed or need, the **opportunity** – a chance to commit a fraud without being caught, and **rationalisation** – being able to justify the criminal act.

The current Covid-19 crisis has led to increases in all areas of the triangle.

With so many people losing their jobs and businesses folding, there will certainly be an **increased pressure** for many to obtain additional funding.

The seasoned criminals will be reliant on reduced staffing levels through sickness, an urgency to obtain medical supplies and different ways of working to supply them with **the opportunity** to exploit systems unnoticed.

With the government already spending £420 billion across 53 different schemes, with some money going to the NHS, some will **rationalise** that there is so much money to be had, their ill obtained windfall will not be noticed.

For many, especially the dedicated, hardworking and committed staff at the NHS, fraudsters taking advantage of this crisis is incomprehensible. But it is happening.

We would ask that you help us in the fight against fraud to the NHS by being vigilant and reporting any concerns to your Local Counter Fraud Specialist. You can contact the LCFS team using the contact details below.

How to Contact your Local Counter Fraud Specialist

If you would like more information or advice about fraud and the latest scams, or to raise a concern please feel free to contact your Local Counter Fraud Specialist. You can find our contact details below:

Steve Moss, Head of Anti-Crime Services	Steven.moss@nhs.net 07717 356 707
Marie Hall, Assistant Anti-Crime Manager	Marie.Hall15@nhs.net 07970 265 017
Rosie Dickinson, Local Counter Fraud Specialist	Rosie.dickinson1@nhs.net 07825 228 175
Olivia Townsend, Local Counter Fraud Specialist	Olivia.Townsend@nhs.net 07717 432 179
Lee Swift, Local Counter Fraud Specialist	Lee.Swift1@nhs.net 07825 110 432
Shaun Fleming, Local Counter Fraud Specialist	Shaunfleming@nhs.net 07970 264 857
Richard Maw, Trainee Anti Crime Specialist	R.maw@nhs.net