Counter Fraud Newsletter – February 2023

AUDIT YORKSHIRE

Current Scam Trends

HMRC releases information to help identify scam phone calls, emails and text messages

In the build-up to the upcoming tax Self Assessment deadline, HMRC has released a useful checklist to help the public decide whether they may have received a spam call, email or text message. The checklist's details are very similar to the advice given by Counter Fraud in all Masterclass and induction materials. Any contact via phone, email, text, WhatsApp, social media etc. could be a scam if it:

- Rushes you,
- Threatens you,
- Is unexpected,
- Asks for personal information,
- Tells you to transfer money, or
- Offers a refund, tax rebate or grant.

Staff members are asked to bear all these red flags in mind when dealing with unsolicited contact via any medium.

If staff members receive a potential scam email, they can report it to spamreports@nhs.net. Suspicious texts can be forwarded to 7726. Staff are also welcome to contact their LCFS (our contact information is on the last page).

Fake vehicle for sale listings

There is a growing trend of fake vehicle sale listings being posted online. People have lost significant sums when they have paid a deposit or the price in full. Others have travelled thousands of miles to bogus addresses, only to find the advert was a scam and they have lost their money.

If you are considering buying a vehicle online, here are our top tips:

- Be wary if the price is too good to be true.
- Popular vehicles will make for a more attractive advert. VW Transporter vans which have a cult following and can be converted into a sleeper vehicle have more fake adverts than any other car or van.
- Check if the photo in the advert has appeared elsewhere (see below for instructions on how to check).
- If the selling site has a built in payment service (Ebay has, Facebook Marketplace doesn't), use this or a credit card rather than a bank transfer as you have more protection if things go wrong.
- See the vehicle in person before paying a deposit. If this is not possible, ask for a live video call and make sure to ask questions (do not accept a pre recorded video).
- Don't feel pressured into buying. Scammers may tell you that other people are interested or willing to pay more to make you act without thinking.

Reverse Image Searches

Fraudsters who post fake listings on selling websites will usually lift photographs of the item from somewhere else. To check whether a photo has been lifted from somewhere else, you can run a reverse image search. To do this:

1. Save the images which have been shared on the suspicious advert.
2. Open the image search on Google (images.google.com)
3. Click on the icon shaped like a camera to run a search using an image.
4. Upload the image that you've saved. You will quickly see if the image has been posted elsewhere.
5. You can also do the same thing to search videos. Just take a screenshot of a distinctive part of the video and run that image through the Google image search.

Can you spare 2 minutes to complete a quick survey on NHS Fraud?

It would really help the Counter Fraud Team if you could take the time to respond. There are only 10 questions and it is estimated that completing the survey should take less than 2 minutes.

To provide your response, please follow this link: https://www.surveymonkey.co.uk/r/K7KZ7MX

Thank you very much for your help.

Scam Trends Continued

Falling for Love or Falling for a Scam: The Dark Side of Online Romance

Not only is love in the air surrounding Valentine's Day in February, so are fraudsters. Please be wary of romance scams on dating sites and social media as these are popular mediums for scammers. Romance fraudsters develop fake identities to build a rapport with their victims, and they can be extremely manipulative and convincing. Once contact has been made, the scammer will quickly seek to move the conversation off the dating app or website and onto personal channels such as WhatsApp or text messages. They do this because they will be targeting multiple people at once and if their account is suspended due to one person reporting them, they will not lose contact with their other victims.

Romance fraudsters have 101 reasons why they can't speak via video call or meet in person. They may claim they are willing to meet up, but don't have enough money to travel. This is often the first way they start trying to take small amounts of money from their victims. Before long, they will say that they need help with a serious issue such as a family or medical emergency, financial problems, or having been the victim of a crime themselves. They then exploit their victim's willingness to help by asking for more and more money. The financial impact of Romance Fraud can be devastating.

You can protect yourself by:

- Keeping conversations on the dating app or website.
- Profile photos may not be genuine, do your research first. Performing a reverse image search on a search engine can find photos that have been taken from somewhere, or someone else (see page 1 for advice on this)
- Never send money to someone you have not met in person, and be very wary about giving money to someone you have only recently started a relationship with.
- If the person asks you to receive money on their behalf, decline. They could be using your account to launder money they have taken from someone else.
- Talk to your family and friends for advice, especially if the person is telling you to keep your new relationship secret.
- Trust your instincts - If you feel like something is wrong, it may well be, so be careful and take a step back.

More advice and information can be found on the Action Fraud website.

Worrying New Twist on the WhatsApp "Hi Mum/Hi Dad" Scam

Last year we shared details of a scam which was targeting people, often over WhatsApp. They would receive a message claiming to be from their son or daughter using a new phone and asking for urgent help paying an overdue bill.

Fraudsters have a new angle – they are now impersonating older relatives. The scam generally takes the form of a message from one of your parents. The message will claim that they are at the shops, have brought the wrong bank card and have had to borrow someone's phone to contact you. They ask for money to be sent to them and promise to pay you back later. Some fraudsters are also using spoofing software, which tricks your phone into displaying your usual contact details, disguising the fact that the message is coming from an unknown sender.

These scams prey on our desire to help our loved ones when we think that they are in trouble. If you receive a text like this, the advice is to verify the request by phone call. Call your relative on an established number first. If you cannot get a reply, you can call the number that has been used to contact you, or request a voice note confirming it really is your relative. Fraudsters will often avoid speaking on the phone, so look out for this red flag. You can read more about this scam on the MSN news website.

Global Increase in Cyber Fraud Attacks During 2022

A report into global cyber attacks in 2022 by Check Point Research (CPR) notes a 38% increase when compared to 2021. Healthcare organisations, along with education and government, were the most commonly targeted. A report they produced earlier in the year identified that the healthcare sector was the most targeted industry in terms of ransomware.

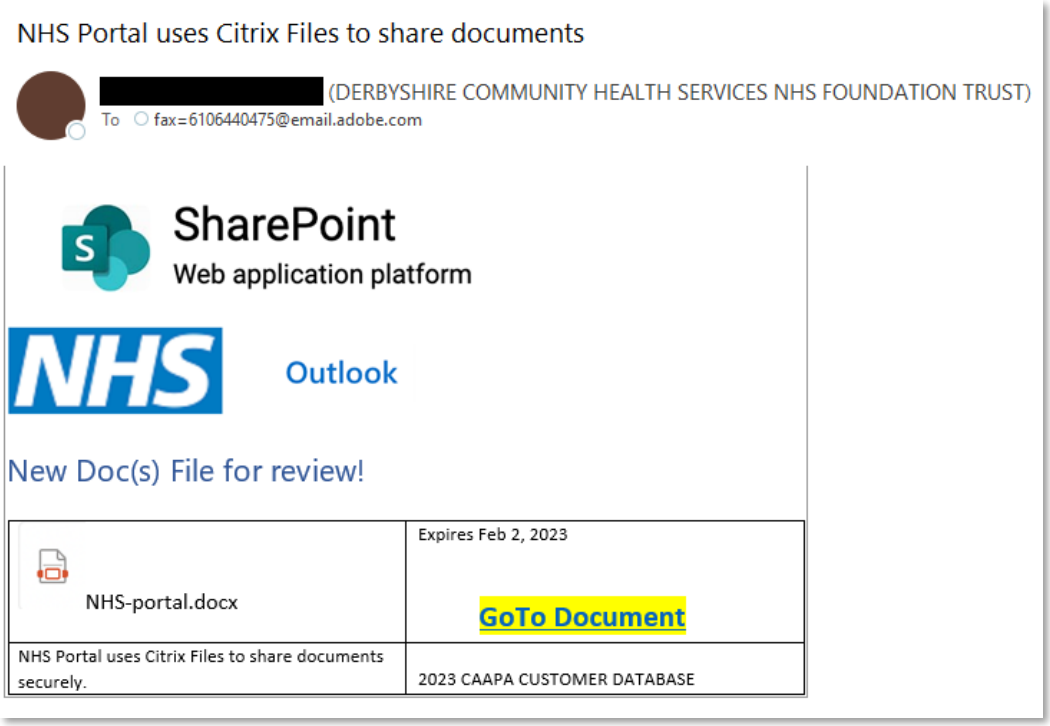
CPR's report stated that Organised Crime Groups (OCGs) responsible for instigating many of these attacks are now believed to be smaller and more agile than before. The OCGs are using business collaboration tools and the rapid shift to online working and learning to provide opportunities for exploitation.

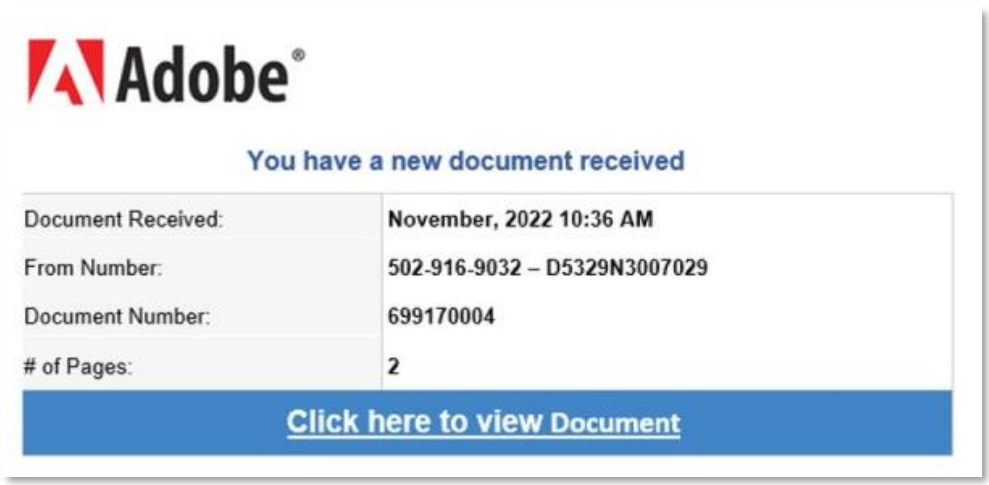
The report points to prevention best practices (rather than detection) as the first area that organisations should consider, to minimise potential exposure to an attack. Their advice includes a focus on cyber security training, ensuring updates are installed, using anti-ransomware technology and avoiding the use of public wi-fi. You can read their full report which contains further advice on the Check Point Research website.

Beware of "Secure File" phishing emails

In recent weeks we've seen a marked increase in the number of "secure file" phishing emails which are being sent to NHS staff. These emails are designed to mimic links to genuine file sharing sites such as Share Point or Yammer. They lift branding from familiar companies such as Microsoft and Adobe to make themselves look more convincing.

They are also typically sent from other NHS.net email accounts which can make them look less suspicious. They are designed to steal your NHS log in credentials by asking you to log in to a scam site , which has been disguised as a legitimate file sharing site.





Avoiding these scams:

1. Never click on links or attachments if you are unsure if they are genuine. You can consider contacting the sender using a safe route (e.g. find their number in the Outlook address book and call them).

2. If you hover over a link in a suspicious email, you will see a small grey box pop up which will tell you where the link is going to take you.

3. If you click on a link and you are then directed to "log in" by providing your NHS email address and password be very cautious. It may be better to seek advice from your LCFS or IT provider.

4. You can forward suspicious emails to spamreports@nhs.net

In the Press

Scammer Jailed for Trying to Steal £2.1m left to Air Ambulance Charity

Stewart Pearman has been jailed for five years and three months for fraud after it was found that he had forged a letter to solicitors in an attempt to falsely inherit over £2.1 million.

Pearman had presented the letter after his friend of 25 years passed away. She had intended to leave the generous sum to an air ambulance charity, which she documented within her will in 2014. She also left Pearman £25,000 and named him as an executor for her will.

Solicitors were suspicious of the letter as it had been created shortly before she died. Her GP has stated she would not have had mental capacity to understand the letter. Two other men admitted that they had been persuaded to provide their own signatures on the letter, falsely signing off a declaration stating that they had witnessed the lady sign the letter. They each received a four month prison term, suspended for 12 months. You can read more about the story on the Independent website.

NHS Fraudster Ordered to Repay £237k

Stephen Day was sentenced to 11 years and 5 months in prison in April 2021, after he pleaded guilty to 10 counts of fraud and 2 of theft. Day's offences included working as a full time Finance Director for three different NHS organisations at the same time. He also defrauded care companies and individuals, with Day believed to have made around £1.3 million through his criminal behaviour.

Day received a Confiscation Order on the 6th of January 2023. This order requires Day to surrender his available assets, which have been valued at around £237k. If he fails to repay within 3 months, an additional 20 months will be added to his prison sentence. You can read more about this story on the CPS website.

Counter Fraud Training

Fraud Prevention Masterclasses

Our Fraud Prevention Masterclass Programme is drawing to a close for this financial year. We would like to thank everyone who has attended and we hope that you found the information you were given useful.

In 2022/23 we covered the following topics:

- Recruitment Fraud
- Cyber Enabled Fraud
- Payroll Fraud
- Creditor Payment Fraud
- Fraud Awareness for Managers
- General Fraud Awareness

We will be publishing a new timetable of Masterclasses in Spring. If you have any suggestions for topics you would like to see covered, we would love to hear from you. Please drop one the Local Counter Fraud Team an email with any feedback or suggestions (our contact details are on the next page).

In the meantime, if you would like to arrange a bespoke fraud training session, or if you'd like us to pop along to your team meeting for a less formal chat about the world of NHS fraud, please don't hesitate to get in touch. You'll find some further details below.

Open offer for bespoke training/fraud awareness input

The counter fraud team is always happy to put together bespoke training for your specific role or department. If your team would benefit from a Fraud Prevention Masterclass on the topics listed above, this can be arranged outside of the planned Masterclass training schedule. We are also happy to attend any team meetings to introduce ourselves and talk about NHS Fraud. If you would like to arrange a session for your team, please contact one of the Local Counter Fraud Specialists (our details are on the next page).

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

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** using our details below. 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 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 my NHS.net email address.

Do not click on any links or attachments.

Forward the suspect email **as an attachment** to **spamreports@nhs.net**. To do this, click on the "More" button which is next to the "Reply, Reply All, Forward" options. Choose "Forward as Attachment".

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 received a suspicious text message

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

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 are below.

How to Contact your Local Counter Fraud Specialist

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
Lee Swift Local Counter Fraud Specialist	Lee.Swift1@nhs.net 07825 110 432
Shaun Fleming Local Counter Fraud Specialist	Shaunfleming@nhs.net 07484 243 063
Nikki Cooper Local Counter Fraud Specialist	Nikki.Cooper1@nhs.net 07872 988 939
Rich Maw Local Counter Fraud Specialist	R.Maw@nhs.net 07771 390 544
NHS Counter Fraud Authority	0800 028 4060 https://cfa.nhs.uk/reportfraud