Counter Fraud Newsletter – November 2022

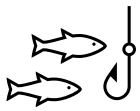
Welcome to the November edition of the Audit Yorkshire Counter Fraud Newsletter for NHS employees. You will find a guide to reporting concerns and contact details for the Local Counter Fraud Specialist team on the last page.

Beware of Black Friday Scams

Fraudsters step up their activity around Black Friday every year. You'll find details of common Black Friday Scams below – remember, if something looks too good to be true, it probably is.

Fake Black Friday Deal Emails and Texts

These messages will tempt you by offering "exclusive" discounts and deals – all you need to do to access the offer is to click on a link…however, the link will take you onto a phishing site which may be a convincing copy of the retailers real website. You will not receive the item you have paid for, leaving you out of pocket and with your personal/financial information in the hands of fraudsters. These scams can be hard to tell apart from genuine marketing materials sent out by retailers.



Some give away signs include:

- The offer is designed to be "unmissable" – they are offering an amazing discount, or access to a product which is sold out everywhere else (such as the latest smart phones, games consoles, or luxury electronics)
- The message claims that to access the offer you must click on a link.
- If you open a browser and visit the retailers official website the offer will not be shown.
- The text or email may also claim that this is a time-limited offer, or that only the first 50 people to order will get the discounted price. This is a tactic to pressure you into acting quickly without thinking it through.
- The message may appear to be from a company you know, but the sender's details are slightly different from their usual contact methods. It may look legitimate at first glance – but doesn't quite match what you'd normally see.
- When you hover over the links in the email, you don't recognise the web address which pops up.
- The message may be from a company you've never previously interacted with or heard of.

Be very cautious of offers that seem "too good to be true". Do not click on links in texts or emails. Instead, go the long way round by opening a browser and navigating to the retailers website, or use their official app if they have one. If you are being pressured to make a quick decision, stop and consider whether you could be being scammed.

Social Media Scams

Posting dodgy deals. Throw away or hijacked accounts may be used to post links to what appear to be amazing deals and discounts. These posts are similar to phishing emails and work by stealing your personal and financial information once you've clicked on the link. Use the steps above to help you spot fake posts.

Competition scams. Social media scammers post fake competitions where you're promised the chance to win a voucher, a prize, or cash. Some brands will run genuine promotions on social media, which makes it trickier to spot the scams.

- Large and well-established brands should have a blue verification tick next to their profile name.
- If it's a smaller brand, have a look at their page and see how long it has been active, what their official website is, whether comments on posts are allowed, and whether there are any reviews on sites such as Trust Pilot.
- If a competition requires you to provide your personal or financial information, please think twice about entering.

Marketplace scams. You may also come across marketplace listings for items that the poster doesn't genuinely hold, or counterfeit items that aren't genuine.

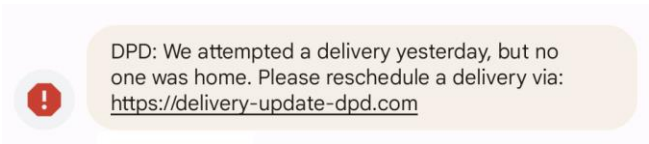
Once they have been paid the item will never arrive, or when it does turn up it will be fake or faulty. The fraudster can quickly close down their social media account and disappear.

- Please be wary of items posted on social media for sale.
- You can use a reverse image search to see if the fraudster has posted someone else's photos of an item.
- You can also ask for more photos or a video of the item – if these can't be provided, alarm bells should be ringing.
- You should not pay for items being sold on social media in advance – if the seller is pressuring you to pay them first then you may be dealing with a scammer.
- It's also worth checking when the sellers profile was first set up – it could be a throw away account that will be deleted as soon as the scam has been carried out.

Parcel Delivery Scams

As we enter the busy shopping period that runs from Black Friday through to the January sales, many people will be placing multiple orders online. As more orders are placed, fraudsters will increase the number of delivery scam messages they send out. These messages are usually sent via text or email. They are designed to mimic messages from genuine delivery companies and will claim that you need to take action in order to receive a delivery. They usually require you to fill in a web form with your personal information and/or to pay a small fee of £1-3 to cover the delivery.

This is often the first part of a more detailed scam. A few days after clicking on the link, the fraudster will ring you up and claim to be from your bank's fraud team. They will use the information you provided on the phishing site and their knowledge of the scam text you received to sound legitimate. They will then try to take more of your money by claiming that your bank balance needs to be transferred into a "safe account" due to the scam text.



If you are expecting a parcel and think you may have missed the delivery, please make contact with the retailer or delivery company directly, using an established contact method. Do not click on links in texts or emails.

If you receive a call claiming to be from your bank, please end the call and use a different phone or wait 30 minutes before calling the bank on their official customer services number. Fraudsters can jam your phone line and although you think you've hung up, when you try to make a new call, you are reconnected to the scammer.

Be Scam Smart this International Fraud Awareness Week

International Fraud Awareness Week (IFAW) ran from the 13th to the 19th of November. This year, we want to draw your attention to Cost of Living scams and how you can keep yourself safe. Fraudsters are quick to take advantage of current events. As people look to reduce their outgoings and access support, there are scam artists out there waiting to pounce.

Cost of living scams that have already been seen include:

- Fake energy bill rebate emails and texts claiming to be from major energy providers,
- Scam texts, emails and phone calls asking recipients to apply for cost-of-living payments,
- Fraudsters calling residents and impersonating local councils asking for bank details to "organise a reduction in council tax"
- Fake supermarket and petrol vouchers being posted on social media and sent via email.

Many of the scams that were popular during the pandemic are likely to be recycled. Since 2020, fraudsters have impersonated major retailers, service providers and even the central government claiming that grants, discounts, or refunds are available due to Covid-19. To access the support, you are asked to share your personal and/or financial information. Fraudsters can easily change the wording of their old scams to mention the Cost of Living instead.

Some top tips for avoiding Cost of Living scams include:

- If you are contacted about a refund, rebate, discount or grant please be extremely cautious.
- To check if an email, text, or phone call is genuine make contact with the organisation using an official customer service route.
- Never rely on the contact details given to you within the message – use Google to find the correct contact route.
- If you receive a suspicious phone call, hang up and either wait for 30 minutes or use a different phone to contact the company using a safe contact route. Never click on links in text messages as you cannot tell where they will take you.
- If you get an email which contains a link, you can hover over the link with your cursor and a small box will appear showing you where the link will take you. If you do not recognise the web address, do not click the link.
- If you are asked to provide your personal details or bank information, please stop and consider if you could be being scammed.
- You can find loads more advice on the Take 5 to Stop Fraud website.
- Consider signing up for our Cyber Enabled Fraud Masterclass - details are on the next page.
- You can contact your LCFS to report concerns about NHS fraud or for advice.

Former Health Care Assistant Who Hid Criminal History to Repay £26k

Narminder Rayat was employed at Worcestershire Health and Care Trust in 2011 and applied for 34 vacancies at the Trust between 2015 and 2016. Although the job application process required her to disclose any relevant criminal history, Rayat did not share that she had previously been convicted of fraud by false representation and fraud by failure to disclose in 2019.

Rayat has been ordered to repay a total of £26,252 to the Trust within 3 months. If she fails to repay the money, she will face 12 months in prison. You can read more about the story on the Express and Star website.

Conviction for Security Guard who Stole and Sold Empty Covid-19 Vaccine Vials

Steven Flint had been working as a security guard for a Covid vaccination site in January and February 2021. During his time there, Flint stole a large quantity of empty Covid vaccination vials which he then sold on eBay. Flint had set up a fresh eBay account, which he registered in the name of an acquaintance to distance himself from the scheme.

The vials remain NHS property even when they are empty. Flint was found guilty of theft at court, and had previously pleaded guilty to fraud by false representation. He was sentenced to one year imprisonment, suspended for 18 months and was ordered to complete 150 hours of unpaid work. You can read more about the story on the Surrey Police 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** (our details will be on your staff intranet and in your organisation's Anti Fraud Policy).

You can also report your concerns to the **NHS Counter Fraud Authority** (0800 028 4060).

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 contact details will be on your staff intranet and in your Anti-Fraud Policy.