Counter Fraud Newsletter November 2023

Welcome to our Counter Fraud newsletter for NHS staff. We hope you find the contents helpful.

International Fraud Awareness Week 2023

The NHS is dedicated to providing world-class healthcare across the UK. To achieve this, it is essential to protect our resources, ensuring they are used for the benefit of patients and the public. International Fraud Awareness Week, which runs from the 13th to the 19th of November, is an opportunity for all of us to unite in safeguarding our NHS against fraudulent activities. When it comes to combatting NHS fraud, every single one of us plays a vital role. Read below for ways you can help in the fight against NHS fraud.

Learn More About Fraud

We understand that not everyone may be familiar with the intricacies of fraud prevention and detection. Therefore, we encourage all staff to reach out to their Local Counter Fraud Specialist for training and support. We run a series of Fraud Prevention Masterclasses (details on page 4) and also offer bespoke training to suit your team's specific needs.

Follow Policies and Procedures

Every NHS organisation has policies and procedures in place to prevent and mitigate fraud. By following these established protocols, you contribute to the creation of a strong, fraud-resistant NHS. Familiarise yourself with these policies, and don't hesitate to ask questions if you have any doubts.

Always Report Suspicions

If you come across anything that raises suspicions of fraud occurring in the NHS, it is your duty to report it. By reporting, you assist us in investigating and addressing any potential threats effectively. A guide to reporting fraud can be found on Page 5 of this newsletter.

International Fraud Awareness Week serves as a reminder of the importance of protecting our NHS from fraud. Let's stand united in our commitment to maintaining the highest standards of healthcare while ensuring the responsible and ethical use of our resources. Together, we can strengthen our defences and make our NHS an even safer place for patients and staff.

Current Scam Trends

Parcel Delivery Scam – new methodology

Several news outlets have recently warned of a new scam in which a parcel is delivered to your home by DPD. The parcel will have your name and address on it. Shortly afterwards, a criminal wearing a DPD uniform will arrive saying there was a mistake and the parcel has been delivered to you in error, and asking for the parcel to be handed back over.

The parcel will contain a high value item such as a brand new mobile phone. Fraudsters have used someone else's bank details to place the order, and then had it delivered to an innocent person's address. This way, there is no trail back to the criminals when the victim reports fraudulent use of their bank card.

Some of the fraudsters have tracked the delivery of the item, and then tried to intercept the delivery driver before they have a chance to knock on the door of the delivery address. You can read more on the Mirror website.

Advice

- DPD have advised that this is a rare scam, but one that they are aware of.
- They encourage anyone who thinks they have been the victim of this scam methodology to report it to Action Fraud.
- They also recommend contacting your bank or credit card provider, and the phone provider.

Booking.com Scams

A new scam is doing the rounds and has been spotted in the wild by one of the counter fraud team. Some customers who have booked hotel accommodation via Booking.com have received emails asking them to provide their card details within 4-24 hours (the amount of time varies) or their booking will be cancelled.

The emails are sent from an official booking.com email address and also appear in the app, making the messages appear genuine. In reality, compromised accounts are being used to send the emails out. You can read more on the Guardian website.

Advice

- Booking.com have advised that if you receive an email and are unsure if you need to take action, you can contact their customer services team around the clock.

- It is best practice to always double check if you are sent any emails asking you to make payments or to supply your bank information.

Protect your Pension

Did you know that the NHS Pension Scheme is changing, meaning that some staff will be able to access more of their pension, at an earlier date than the scheme allowed before? The changes took effect on 1st October 2023 for anyone who was in the pension scheme on or before 31st March 2012.

If this applies to you and you take up the opportunity to access your pension early, or if you are due to take your pension soon, please be aware that fraudsters could be in waiting ready to commit pension fraud.

Fraudsters use a range of methods including phone calls and online tactics to try and part people from their hard-earned cash. These could be emails, social media posts or offers for a ‘free pensions review’.

Cold calling about pensions is illegal, but this doesn’t deter a fraudster, who might be calling from anywhere in the world. They may try to convince you of a ‘pensions loophole’ or try to sell you a ‘one-off investment’, or use words like ‘pension liberation’. These phrases are red flags, as is the urgent manner in which they might speak – this is more likely due to them being in a call centre where they are trying to con as many people as they can in a day.

Advice

If you are approached by someone you don’t know, to ‘get help’ with how the new changes might affect you, please remember that all options will be explained by NHS Pensions directly.

There is no need to pay a company to help you make your pension choice.

NHS Pensions will automatically contact all eligible members as soon as it is possible and will give you the information you need to help you make your decision at retirement.

For details from NHS Pensions directly please see the NHSBSA website. You can get advice on avoiding pensions scams on the Pensions Regulator website.

Cyber Security

Hacked Facebook Accounts

Facebook holds a wealth of information about you which is great news for fraudsters. Hackers may guess your password, or get you to inadvertently reveal it by sending phishing emails. Your password may also be revealed in a data breach.

Hacked accounts can be used for lots of different purposes. For example, the fraudster may use your account to target your contact list with scam messages and dodgy offers.

We have also been told about people's hijacked social media accounts being used to post fake listings in Facebook Marketplace. Doing this allows the fraudster to look like they're someone who has held a profile for a long time, as accounts that have no connections or are very new may be spotted if posting fake listings. It also provides a false lead if the matter is investigated, and can lead to ripped-off customers directing their anger at the wrong person.

Having your account hacked is a stressful and worrying experience. Below, you'll find our top tips on what to do if you think your account has been compromised.

If you think your Facebook has been hacked, we suggest taking the following steps….

1. Go into Settings & Privacy > Settings > Activity Log > Where you're logged in. Look out for any log ins on unfamiliar devices or locations. Next to any unrecognised log in, click the three vertical dots. This will then give you the option to log out of this particular session.

2. Change your password. If this has been done by the intruder (to block you out), click on the Forgot Your Password link (under your Facebook login). You will then be asked to verify yourself, such as providing the email address or phone number linked to the account.

3. Create a post to alert your Facebook Friends that you have been compromised and not to trust any links or apps which look like they have come from you.

4. Go into the Settings menu and click on Apps. Delete any which you do not recognise – they may be malicious.

5. Going forward, if you haven't done so already, you can change your settings so that you receive an alert when there is a new log in on Facebook. Go to Settings > Password and Security > Login alerts.

6. Turn on multifactor authentication. This means that even if your password is stolen, nobody else can access your Facebook without your knowledge. To activate this, go into Settings and Privacy > Settings > Security and Login > Use two-factor authentication

7. If your personal account is connected to any work related Facebook pages / Facebook adverts, alert admin immediately.

Facebook have a reporting tool which can be accessed here - https://www.facebook.com/hacked/

Alternatively, log onto Facebook and search for “hacked” to be directed to the Secure Your Account help page.

On a related note, missing person / pet Facebook appeals...

On Facebook you may have seen posts relating to missing pets or vulnerable people being missing from home. Social media can be a very useful tool in raising awareness and ensuring people keep an eye out, and many of the posts are genuine.

However, there has been an increase in spoof posts of this nature. The posts are circulated far and wide, with the fraudster posting the same content across the globe, but claiming the person or pet has gone missing locally. The ability to leave comments on these posts is always switched off.

The purpose of these posts is to gather a high number of likes and shares. Comments are switched off to stop anyone from mentioning that the post isn’t genuine. Once the post has enough popularity, it is edited to be about something completely different. Commonly, they will be turned into posts linking to phishing websites, fake products, or investment scams. Please try to verify posts before sharing them - check whether comments can be left, if the account posting the appeal is genuine (e.g. local policing teams may post genuine appeals), and if in doubt, do not interact with the post.

Black Friday 2023

It’s that time of year again! The period between Black Friday and the January sales is an extremely busy time for fraudsters.

With so many of us searching for deals ahead of the festive period, and hoping to snap up a bargain in the new year, fraudsters are always lurking behind the scenes. Last year, £10 million was lost to fraud during the festive shopping period, and those aged 25-34 years old were most likely to be victims.

The National Cyber Security Centre has published an article encouraging all shoppers to be aware of the increased risk.

There are lots of different methods a cyber-criminal may use at this time of year. Some of the common tactics they use include:

- **Phishing –** The fraudster contacts you, pretending to be a brand you recognise. They offer unbelievable discounts - all you need to do is click on a link. The link takes you to a phishing site where your card details are stolen.

- **Fake Listings -** The fraudster creates a fake listing for that “must-have” gift on a social media marketplace. They ask for payment up front. Once you have paid they block you. They use a throw-away account, or a real profile that has been hijacked.

- **Parcel Scams -** You get a text message saying you need to pay £2 to cover missing postage, or to rearrange a missed delivery. You click the link and pay. Your card details are harvested. A few days later, the fraudster calls pretending to be from your bank’s fraud team. They ask you to move your money to a “safe” account.

Keeping yourself safe

- With emails and texts, check sender’s details closely. If in doubt, do not click on any links or attachments.

- If you are expecting a parcel and you're not sure if a text / email relating to a delivery is genuine, get in touch with the retailer and ask for tracking information.
- Watch out for pressure tactics like false deadlines and "limited quantity available" warnings. Although these can be genuine sales tactics, they can also be used by fraudsters to panic you into buying without thinking it through.
- Deals that look "too good to be true" are best avoided.
- Check TrustPilot and other sources for reviews whilst shopping.
- There are loads of different marketplace scams. For further information and advice, please see this article on the Reader's Digest website.
- Where possible, use your credit card to place orders as these have more protection. Don't pay by bank transfer.
- Remember - if in doubt, don't shell out!

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 or not it is fraud related.
You are very welcome to contact your Local Counter Fraud Specialist for advice and support, our details are below.

How to Contact Your Local Counter Fraud Specialist:

Your Local Counter Fraud Specialist is: