MAY 2024

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

Welcome to our Counter Fraud newsletter for NHS staff. We hope you find the contents helpful. If you need any advice on fighting NHS fraud, you can find our contact details in your organisation's Anti-Fraud, Bribery and Corruption Policy.

IN THIS EDITION

Government Fraud Detection Tool

The Government are continuing to fight fraud against the public sector with technology. They are increasing the data which is input into their fraud detection tool, SNAP (Single Network Analytics Platform). SNAP uses Artificial Intelligence to analyse public sector data. In March 24, new datasets were added to the database to increase the scope of detecting fraud.

This included 647,000 companies in the UK who do not have any declared income. The NHS are frequently contacted by illegitimate suppliers and removing the fake companies may help to stop this.

Sanctions and debartment (where a company has been stopped from undertaking business due to mismanagement, including fraud) have also been added to SNAP which will help to identify suspicious networks and organised crime.

This innovative technology will help to detect and deter criminal activity which will free up resources for public services.

Gifts and Hospitality Reminder

NHS staff are expected to uphold the Nolan principles, including selflessness, openness and integrity. Similarly, all NHS bodies are expected to put policies in procedures in place to reduce the risk of fraud, bribery and corruption.

It is therefore essential that staff understand what is expected when it comes to offers of gifts and hospitality at work. Organisations may set different limits around what can be accepted, as well as having different ways of recording gifts and hospitality.

This information is usually covered within your organisation's Conflicts of Interest Policy, Standards of Business Conduct Policy, or within a specific Gifts and Hospitality Policy.

If you are unsure where to find this information, please speak to your Local Counter Fraud Specialist and we will help you to find the right policy.

Scam Trends

Ticket Fraud

Action Fraud, the national fraud and cybercrime reporting service, has launched a ticket fraud awareness campaign, warning people to be alert to fraudsters trying to defraud people planning for popular events.

With festival season on the horizon, concert goers looking to get last minute tickets to this summer's top events are urged to be on their guard against fraudulent sellers.

Last year more than 8,700 people reported they had been a victim of ticket fraud, with a total of £6.7 million lost. This works out to an average loss of £772 per victim.

The warning comes ahead of the Glastonbury Festival ticket resale and before top summer events, such as Taylor Swift's sell out Eras tour.

Of the reports made to Action Fraud last year, 34% of reports (2,993) mentioned concert tickets, 29% of reports (2,523) mentioned travel and 18% of reports (1,561) mentioned sporting events.

Acton Fraud's advice on how to protect yourself from ticket fraud:

- Only buy tickets from the venue's box office, the promoter, an official agent or a well-known and reputable ticket exchange site.
- Avoid paying for tickets by bank transfer, especially if buying from someone unknown. Credit card or payment services such as PayPal give you a better chance of recovering the money if you become a victim of fraud.
- The password you use for your email account, as well as any other accounts you use to purchase tickets, should be different from all your other passwords. Use three random words to create a strong and memorable password, and enable 2-step verification (aka Multi Factor Authentication).
- Be wary of unsolicited emails, texts or adverts offering unbelievably good deals on tickets.
- Is the vendor a member of Society of Ticket Agents and Retailers (STAR)? If they are, the company has signed up to their strict governing standards. STAR also offers an approved Alternative Dispute Resolution service to help customers with outstanding complaints. For more information visit star.org.uk/buy_safe.

Fraudsters often create fake ticket retail companies. Victims are lured in using social media or phishing emails with offers of the chance to buy tickets to a popular event, but instead give away their personal information or money, with no tickets received in return. Phishing messages often look real, but instead will either steal your information or divert to malicious websites which can infect your computer with malware.

If you feel at all suspicious, report the email to the Suspicious Email Reporting Service (SERS) at report@phishing.gov.uk.

For more advice on how to stay secure online, please visit the Cyber Aware page on the National Cyber Security Centre website.

Find out how to protect yourself from fraud: https://stopthinkfraud.campaign.gov.uk

If you live in England, Wales and Northern Ireland and have been a victim of fraud or cybercrime, report it at www.actionfraud.police.uk or by calling 0300 123 2040

Identity Fraud

The Independent has recently covered the story of a man whose identity was stolen by fraudsters and used to run up over £17,000+ of debt. The story highlights the importance of protecting your personal information.

Identity theft is when criminals steal your personal information.
Identity fraud is when they use your stolen information to impersonate you.

They may use your details for a variety of purposes including:

- Opening bank accounts,
- Applying for credit cards,
- Obtaining official documents such as passports / driving licences,
- Setting up financial agreements such as phone contracts or car finance.

Identity theft can occur in lots of different ways, and victims often don't find out exactly how their details were compromised. Potential routes to identity theft include missing / stolen documents, a data breach, phishing emails / text messages that trick you into sharing your details, and criminals intercepting discarded documents.

Fortunately, there are things you can do to reduce the risk of identity theft / fraud.

- Make sure you know where key documents such as your passport and driving licence are.
- If your identity documents go missing make sure you report it to the passport office / DVLA.
- If you keep paper documents such as credit card statements, utility bills, or payslips, make sure you store them in a secure place.
- Don't put things such as packaging, circulars or letters in the bin without removing your personal information first.
- Use a secure method such as shredding if you are getting rid of documents which feature your personal information.
- Regularly check your bank statements and alert your bank to any payments you don't recognise. Often fraudsters will start with small payments to see if these are spotted before making higher value purchases.
- If you move house, make sure you update anyone who holds your personal information. You can also contact Royal Mail to temporarily redirect your mail to your new address.
- Be wary of unsolicited emails and text messages, especially if they contain links or ask for personal information.
- Use strong and unique passwords for your online accounts.
- Check if your accounts have been involved in any data breaches by visiting Have I Been Pwned? The website will provide advice on what to do if there have been any data leaks. It is best practice to update your passwords and enable Multi Factor Authentication wherever possible.

If you think you have been the victim of identity fraud, the Home Office have produced a useful checklist which explains steps you can take: Identity fraud victims' checklist (actionfraud.police.uk)

Phone Upgrade Scam Warning

Humberside Police have warned the public about a phone upgrade scam doing the rounds. Fraudsters cold call potential victims, pretending to be from legitimate phone companies. The fraudster will offer a free upgrade, or a deal on a new handset which is too good to refuse.

Under the guise of arranging the "upgrade", the fraudster will ask the victim for personal and financial details. They use these details to request an upgrade on the victim's real account, but arrange for the wrong handset to be delivered.

Using parcel tracking info, the fraudster waits until the victim receives the phone before calling again to apologise that the wrong handset has been dispatched. They advise the victim to send the phone to an address so that the correct handset can be sent. Of course, no replacement handset will appear.

The fraudster has used the victim's details to get hold of a brand new phone with the victim footing the monthly bill.

- Please be wary of cold calls. If in doubt, hang up, and contact the company on an established customer services number.
- If you receive an item in error, contact the sender as soon as possible using official contact details.
- Remember, deals that sound or look "too good to be true" can hide nasty surprises.

You can learn more about this scam and how to protect yourself on the Action Fraud website.

REPORTING FRAUD CONCERNS

Fraud vs the NHS

If you think that fraud may be being carried out against the NHS, please **notify your Local Counter Fraud Specialist**. You'll find our contact details in your organisation's Anti-Fraud, Bribery and Corruption Policy,.

You can also report your concerns to the **NHS Counter Fraud Authority** using their online reporting tool or phone number: 0800 028 40 60.

If you choose to make an anonymous report, please give as much information as possible as we won't be able to get back in touch with you to clarify anything.

Suspicious Emails

Do not click on any links or attachments.

If you have received a suspicious email to your **@nhs.net** email account, you can forward it (as an attachment) to **spamreports@nhs.net**

If you are not sure how to forward an email as an attachment, contact the LCFS team and we will help you.

If you have been sent a suspicious email to another type of email account (not @nhs.net) you can forward it to **report@phishing.gov.uk**

Suspicious texts

Do not click on any links in the suspicious text message.

You can forward suspect text messages to 7726.

Fraud against a member of the public

These concerns can be reported to **Action Fraud (0300 123 20 40),**

If the person has lost money, it may also be appropriate to report the matter to **the police.**

If you suspect that the person's bank account has been compromised, it is important that they **speak to their bank** as a matter of urgency.

I've read the options but I'm still not sure what to do

The Local Counter Fraud team will be happy to advise.

Our contact details can be found in your organisation's Anti-Fraud, Bribery and Corruption Policy.