Counter Fraud Newsletter – March 2022

Welcome to the March 2022 edition of our Counter Fraud Newsletter for NHS staff. Please feel free to contact your Local Counter Fraud Specialist for advice on any type of fraud, you will find our details on the last page.

Current Scam Trends

Online Voucher Scam
We have been made aware that a senior NHS employee was recently targeted by cyber criminals who impersonated another member of staff via email. The criminal claimed to be a known colleague, and asked the senior member of staff to purchase some Google vouchers due to technical difficulties they said they were having. They stated that they would pay the senior staff member back later.

The email was written with a friendly and conversational tone, to try and make the message seem like it could be genuine. The senior employee called their colleague and was able to check that they had not sent the email.

Please be cautious if you receive any emails that ask you to make unexpected or unusual purchases. Verify the request with the apparent sender to check if it is genuine, using existing contact information (don't rely on any contact info which is given within the email you've been sent).

If in doubt, you can contact your Local Counter Fraud Specialist for support and advice.

Tax fraud scam
As tax returns deadlines loom, fraudsters are busy trying to pocket fake tax refunds by obtaining your personal details, such as Government Gateway log ins, and submitting fake Tax Self-Assessment claims in your name.

One way the criminals have been doing this is by getting you on board. There have been adverts on some social media sites asking to 'borrow' your identity in exchange for a share of the money obtained in the bogus tax refund, which is advertised as being 'risk-free'.

Getting involved in tax fraud is obviously never a good idea, but conspirators are getting more than they bargained for when they realise that once fraudsters have their Government Gateway log in, they can also access details used to set it up, such as ID documents and bank account info.

You can report tax fraud concerns to the HMRC here: Report fraud to HMRC - GOV.UK (www.gov.uk)

Holiday Scam Warning
With the return to (hopefully) warmer weather, many of us will be thinking about booking a break to look forward to. Unfortunately, fraudsters look to capitalise on this by setting up fake holiday listings to con people out of their hard earned cash. So, what signs can you look out for?

- Watch out for deals that seem too good to be true. We all love a bargain, and fraudsters are quick to promise unbelievable offers. The offers are unbelievable, because the fraudster has no intention of delivering what they've advertised.
- Often, these offers will be accompanied by pressure tactics—the listing will state that the

deal must be booked immediately, and/or it is only available to the first 100 customers who sign up.

- It is easy to mix these pressure tactics up with standard sales tactics. Don't let anyone panic you into handing over your financial details. Take your time to check the facts.
- Research the company to look for signs they may be fraudsters. Established holiday companies should have a proper online presence. You should be able to find reviews from other customers, company registration details, ABTA/ATOL protection numbers, and clear booking/cancellation/complaints procedures. If something doesn't feel right, then the chances are that something isn't right.
- Fraudsters have been known to steal images and information from genuine properties that they have no rights or access to. They then create fake listings on sites such as Airbnb to try and entice holiday makers. A tell-tale sign is that the "host" will ask you to pay them for the booking outside of the official website or app. You should always pay via the official app or website. Avoid booking with people who ask you to pay by bank transfer only.

You can read more about avoiding holiday scams by checking out this article on the Which website. You can also get more advice about keeping yourself safe on holiday (as well as during the booking process) by visiting the Take 5 To Stop Fraud website.

Donating Safely to Assist Ukraine

The Charity Commission and Fundraising Regulator have urged the public to 'give safely' to registered charities as people make generous donations to causes helping to support and protect people affected by the invasion of Ukraine. By giving to a **registered, regulated** charity, you can have assurance that your donation will be accounted for in line with charity legislation. Established charities with experience of responding to disasters are usually best placed to reach victims on the ground.

People looking to donate to causes working in Ukraine and neighbouring countries, can and should make a few simple checks before giving, to avoid fraud:

- Check the charity's name and registration number at government charity check link. Most charities with an annual income of £5,000 or more must be registered, and you can use the advanced search function to identify charities working in specific regions and countries
- Make sure the charity is genuine before giving any financial information- see above.
- Be careful when responding to emails or clicking on links within them.
- Contact or find out more online about the charity that you're seeking to donate to, to understand how they are spending their funds.
- Look out for the Fundraising Badge on charity fundraising materials, this is the logo which shows that a charity has committed to fundraise in line with the Code of Fundraising Practice.
- Finally, don't feel pressured to give more than you can afford.

While no one should be dissuaded from giving to charity, these simple steps can ensure that the money donated goes to the right place.

Cyber Security – Watch Out for Ransomware

Researchers at SonicWall, a cybersecurity company, found that the volume of ransomware attacks on their customers rose by 105% in the last year with 623.3 million attempts recorded in 2021.

Ransomware is a type of malicious software (malware) which locks your files and accounts, and demands that a ransom is paid in order for you to reclaim access. .

The NHS and NCSC do not recommend paying ransom demands, as doing so tells the cyber criminals that their crime pays. Criminals may also attempt to blackmail their victims with the threat of releasing the data they've stolen. Avoiding ransomware is therefore extremely important.

To protect yourself and your organisation from Ransomware:

- Do not click on unexpected links and attachments. Verify that the sender is legitimate and that they intended to send you the link/attachment (their email account may have been hijacked and they may be unaware that you've been sent anything).
- To find a safe contact route, do not rely on information provided within the email. If the person is from within the NHS, consider whether you can call them on Microsoft Teams, look up their phone number in the Outlook directory/on the intranet, or if one of their colleagues can give you their most up to date contact information. If they are from an external organisation, use Google to search for their company's generic customer services email address or phone number.
- Hover over links before clicking on them. You will see a small box pop up that shows you where the link will take you. Links may look innocent on the surface, but could have a hidden agenda.
- Switch off your device at the end of every day to ensure that updates are installed.
- Make sure you are using unique passwords for each account. If you rely on one password and it is compromised, fraudsters could seize control of all of your accounts and demand payment.
- Consider activating Multi Factor Authentication wherever it is available. This provides a really good level of protection to your accounts. If a cyber criminal does manage to steal your password, they won't be able to get in without providing the second layer of authorisation.
- If you have to use public Wi-Fi, make sure you activate a VPN on your device before connecting. It is remarkably easy to create a fake Wi-Fi hot spot, and genuine public Wi-Fi networks can still be used to target anyone who connects to them.

Please be vigilant and contact your LCFS for advice if you have concerns. You can read more about Ransomware on the National Cyber Security Centre website.

In the Press

Suspended Sentence for Fraudster Who Conned His Way into NHS Employment

Mohammed Bashir was found guilty of fraud at Bolton Magistrates' Court in February, and has been handed a sentence of 28 weeks imprisonment (suspended for 2 years). Bashir had falsely claimed to hold a Security Industry Authority Licence, an important document which he did not

possess. He was ineligible to apply for a licence due to his conviction history, which includes convictions for dishonesty, drugs offences, driving offences and a violent offence.

To bypass this, Bashir had used a licence held by his father to make it appear that he was appropriately registered. By doing so, Bashir had managed to secure a role at a security firm. This firm provided security services to the NHS. This led to Bashir working on a number of NHS wards in the North West between December 2018 and February 2019.

As well as receiving a suspended sentence, Bashir has been ordered to pay £1,000 in prosecution costs and a £128 victim surcharge. You can read more about this story on the Bolton News website

NHS Scam Texts Already Responsible for £880,000 of loss in 2022

An article published in the i newspaper focuses on a new report from Santander. The report reveals that consumers have already lost £880,000 to NHS scam texts in the first three months of 2022.

Details of this scam have been included in previous editions of the newsletter. As a reminder, the texts are designed to look as though they've come from the NHS. They warn the recipient that they've been in contact with a confirmed Covid-19 case, and direct them to click on a dodgy link to "order a test".

A small payment is requested (allegedly to cover postage) as well as "confirmation" of the recipient's name, address and date of birth. This is all about collecting the financial and personal details of the recipient. They are then contacted at a later date by a fraudster who claims to be calling from their bank's fraud team. The caller sounds plausible as they've got lots of information they can quote. They then set about convincing the victim to transfer their money into a "safe" account which is controlled by the fraudster.

Please remember to be very cautious when dealing with texts that contain links. Remember that banks will not ask you to transfer money to "safe accounts". If you are called by someone claiming to be from your bank, hang up and use a separate phone line to contact the customer services team of your bank (their number is on the back of your bank card, or use Google to find the number online).

Counter Fraud Training

The Counter Fraud team are always happy to deliver training and awareness work to staff. This can be in whichever format your team would find most helpful.

We are happy to put together bespoke training to suit your area of work and the risks you're most likely to face during your day-to-day role.

We are also happy to drop into team meetings to introduce ourselves and to give an informal overview of fraud risks affecting the NHS.

If you would like to access any of the above, please don't hesitate to get in touch with a member of the Local Counter Fraud team.

2022/23 Masterclasses

The Local Counter Fraud Team are putting the 2022/23 Fraud Prevention Masterclass programme together. We will be adding two new modules onto the programme, General Fraud Awareness which will be suitable for all staff, and Fraud Awareness for Managers. In addition, the Cyber Enabled Fraud Prevention Masterclass that was available in December 2021 will be added into the regular programme so that more staff can access it.

If you have any suggestions of topics that you'd like us to cover, you're very welcome to get in touch and let us know. You can find our contact details in the section below.

Request for Newsletter Feedback

We would be really grateful if you could let us know what you think of this newsletter, including any suggestions for content or amendments. Our grateful thanks to one of our readers who suggested more information on reporting routes - we hope the information below covers the options available to you. If you can spare 5 minutes to fill out the link below, it would be much appreciated. You can also email rosie.dickinson1@nhs.net. You can find the Survey here: newsletter feedback survey

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 make 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 this 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:

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:

Nikki Cooper, Lead Local Counter Fraud Specialist	**nikki.cooper1@nhs.net** **07872 988 939**
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
Richard Maw, Local Counter Fraud Specialist	r.maw@nhs.net 07771 390544
NHS Counter Fraud Authority Fraud and Corruption Reporting Line	0800 028 4060 NHS Counter Fraud Authority Fraud and Corruption Reporting Line