Counter Fraud Newsletter – January 2022

Welcome to the January 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

Romance Fraud

As Valentine's Day approaches, regional police forces are advising the public to be wary of romance fraudsters on dating sites and social media. These criminals develop fake identities that they use to build a rapport with their victims, and they can be extremely manipulative and convincing.

Once contact has been made, the fraudster will quickly seek to move their conversation off the dating app or website and onto personal channels such as WhatsApp. This is because they will be targeting multiple people at once, and if their account is suspended once one person reports them, they won't 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; with Action Fraud data finding that almost £92 million was lost to these scams in a single year.

You can protect yourself by:

- Keeping conversations on the dating app or website.
- 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.

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

Fake Police Officer Phone Calls

North Yorkshire Police have warned the public to be vigilant after they received three reports of fake police officer phone calls being received in a 24 hour period. The fake police officer scam tends to pop up every so often and has remained popular during the pandemic. Over the last few months, members of the public have reported receiving calls from people claiming to be police officers and notifying them to a problem with their bank account. The caller will usually claim that an individual has been arrested with a cloned copy of the victim's card, a drug dealing gang has been using their account to launder money, or a family member (usually a "grandson") has been arrested trying to use their card.

If calls of this nature are received, the public are advised to:

- Do not share any financial details with people who call you out of the blue, even if they claim to be from the police. Ask the officer for their name, rank, police force and collar number and write these down.
- Take a note of any details you can see on your caller ID (e.g. phone number being used)
- End the call and ring a family member so you can check that your line has been cleared

- Use 101 to connect to the relevant police force and check the callers identity.
- If you think you have given your financial details to a fraudster, contact your bank immediately.

Sim Swapping Scams

SIM swapping occurs when a genuine phone number is cloned onto a new SIM card. By doing this, a fraudster can gain access to sensitive information linked to your mobile phone.

To carry out this scam, the fraudster may impersonate your mobile phone network provider, and claim that you need to arrange a new SIM card. They'll send you a text or email to make it look like this is something you need to do. If you follow the links and instructions provided, you will hand over control of your mobile phone.

Alternatively, you might not hear from the fraudster at all. Instead, they use data they have gathered about you using social media, data breaches, and online accounts to impersonate you. They contact your mobile phone provider and ask for a SIM swap.

Once this has been done, the fraudster has the ability to intercept your calls and texts, as well as security codes generated by your mobile banking service and other online shopping accounts. The first signs that your SIM has been swapped tend to include:

- Loss of function on your phone - e.g. you can no longer make calls or send texts.
- Notification of activity elsewhere - a message saying your number has been activated on a new device.
- Loss of access to online accounts - e.g. you can no longer get into your mobile banking using your usual access credentials.

If you find that your phone suddenly stops working, or if you get a message saying your phone number has been activated on a different device, notify your bank and your mobile network provider immediately.

Be careful of the information you share on social media. Fraudsters use social media to gather background information that may help them to answer security questions for your accounts. Make sure you use good security settings to protect your information.

You can also increase your security by ensuring you set strong passwords (see this article on the National Cyber Security Centre website for advice).

Cyber Security – Reverse Image Searching

If you're not sure if an image you've been sent is genuine, you can check online to see if it has been posted elsewhere.

This is helpful if you're concerned that someone is impersonating another person (as explored in the Romance Fraud article on the first page). It can also come in handy if you're trying to verify whether a website or item listed for sale is genuine. You will be able to find out if the photos which are being used are likely to belong to another company or retailer.

To reverse image search, you can follow the 5 steps below:

- First, save a copy of the photo you want to check onto your desktop.

- Then, open your web browser and head to Google. In the top right of the screen you'll see the option to open Google Images.
- When you've clicked on images, you'll see the search bar in the middle of your screen. Instead of typing in your search terms, click on the little icon shaped like a camera.
- Click "upload image", then "choose file", then select the image you saved onto your desktop.
- You will then be able to see if the image you've searched for has been used elsewhere online.

It is easier to reverse image search using a desktop or laptop computer. You can use your mobile phone or tablet, but the method will be a bit different. The instructions vary depending on the type of device and the operating system being used.

If you want to find out how to do this on another device, simply use a search engine to find the right instructions that will work for your device.

In the Press

Paramedics who posed as nurses to steal medication jailed

Two paramedics who impersonated nurses to persuade terminally ill patients and bereaved family members to hand over medication have been jailed for 5 years.

Ruth Lambert and Jessica Silvester were both paramedics working in Kent when they committed their offences.

Enquiries demonstrated that they had abused their access to NHS systems to deliberately target patients who were on end-of-life care packages.

The pair had bought nurses uniforms that they would wear whilst carrying out their crimes. Their M/O included persuading vulnerable patients to hand over their medication, and visiting newly bereaved families to "collect" left over medicine which had not been used by their loved one.

Lambert and Silvester both pleaded guilty to conspiring to burgle and conspiring to commit theft. They have each been sentenced to 5 years in prison.

They have also both been suspended from the official Health and Care Professions Council register.

You can read more about the case by following this link: [Secamb paramedics stole medication from dying patients - BBC News]

HMRC Recovers over £1 billion from Fraudsters

Since the introduction of the HMRC Fraud Investigation Service 5 years ago, over £1 billion has been recovered from fraudsters.

The Fraud Investigation Service has proactively sought to recover the proceeds of crime, by using the Proceeds of Crime Act. This piece of legislation allows financial assets which have been gathered through criminal activity to be recovered, with the money returning to the public purse.

The confiscation work has included interesting and unusual recoveries, including £750,000 of gold bars and £48,000 which had been hidden in a criminals freezer.

You can read more about the work of the [HMRC Fraud Investigation Service here.]

Did You Know? Secondary Employment

The Counter Fraud Team receives more referrals about Secondary Working than any other topic.

Having more than one job is certainly not illegal; however, any employee who is considering working elsewhere (or who already works elsewhere) must consult their line manager in line with the Standards of Business Conduct Policy, Secondary Employment Policy, and/or Conflicts of Interest Policy in place at their organisation. This requirement is also often reflected in NHS contracts of employment.

The fraud team is most commonly notified of concerns where a member of NHS staff has been signed off sick from their substantive post, and is believed to have been working elsewhere during their sick leave. This doesn't always constitute a fraud offence - the specific circumstances are really important.

- If you are signed off sick from your NHS role, and intend to carry out any other work during your sick leave, you must notify your line manager.
- If you need to present a fit note to cover your absence, you must also make sure that you inform your GP of your other role so that they can consider whether you are fit to carry out that role or not. They can then cover this on your fit note.

It is also vital that you consider whether your secondary role could present a Conflict of Interest for you in your NHS role. Potential conflicts of interest must be declared.

- You can find instructions on how to make a declaration this within your organisations Standards of Business Conduct Policy or Conflicts of Interest Policy.
- If you are in any doubt as to whether something needs to be declared, make a declaration.

Occupational Health and HR can also provide support and guidance around these issues.

If you manage people and would like further information or to attend a fraud awareness workshop, please contact your LCFS.

Counter Fraud Training

The LCFS team are continuing to deliver our series of Fraud Prevention Masterclasses for NHS staff, covering key fraud risks within different areas.

The masterclasses are delivered via Microsoft Teams and last around 45 minutes to 1 hour.

The sessions have been delivered on a monthly basis, and cover some key areas that have specific fraud risks. They include an overview of the various risks which may be encountered, real life case studies and practical advice on the prevention of fraud risks.

If you have an interest in any of the topics below and would like to sign up for a session, please get in touch with Rosie Dickinson (rosie.dickinson1@nhs.net)

The final Masterclasses for 2021/22 are as follows:

- Recruitment Fraud – 10am-11am, 4th February
- Creditor Payments – 10am-11am, 18th February
- Payroll Fraud – 10am-11am, 11th February

Our Masterclass programme is now winding down for 2021/22, however we will be running more sessions in 2022/23.

If you have any suggestions or requests of other topics you would like us to cover in the next set of masterclasses, or to join the waiting list for next year's programme, please don't hesitate to get in touch with any of the Local Counter Fraud Team (our contact info is below).

Your Local Counter Fraud Specialist is:

Nikki Cooper
nikki.cooper1@nhs.net
Mobile 07872 988 939