Counter Fraud Newsletter – July 2022

Welcome to the July 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.

Current Scam Trends

"Underpaid Tax" Scam targeting Overseas Nursing Staff

We have been advised of local overseas nursing staff being contacted by someone claiming to be from Gov.uk. The caller states that the hospital the recipient works for has made a mistake with their tax and that they owe between £1,000 and £2,000. The caller claims this must be paid otherwise the nurse will be arrested and prosecuted.

Alarmingly the callers have known that the staff were part of an overseas nurses group. They also knew the victim's names and where they originated from. The caller provided the telephone number for Birmingham Crown Court (0121 681 3300) and the same number has been shown at the top of WhatsApp messages sent by the scammers.

HMRC and Gov.uk have messages on their websites reminding everyone that they will never contact you to ask for payment over the phone. If you do receive a call and you're unsure if it is genuine, please hang up without sharing your personal or financial details. For more details please see the GOV.UK website.

Amazon "iPhone" order scam

A new scam which is designed to hijack your Amazon account has been reported. Victims will receive a phone call from someone who claims to be calling from Amazon. The callers says that they are phoning to report that the person's Amazon account has been compromised, and has been used to order an iPhone. The caller will ask if the victim wants to cancel this order. If they agree, the caller says they will send a "one time password" to facilitate the cancellation.

A text message containing a 6 digit code from Amazon will then arrive. The caller will ask the victim to read the code out loud. The text message and code are genuine, and are generated when an Amazon customer requests a password reset.

If the code is shared with the caller, the scammer can then log in and change the victim's Amazon password, locking them out. The account can then be used to place orders using the victims saved card details.

It has been reported that these scam callers do not know the victims name. Several potential victims have asked the scam callers to confirm what their name is, or what name is on the Amazon account. The scam callers have been unable to answer, and therefore the potential victims were able to avoid their account being hijacked.

Please be wary of calls of this nature. You should hang up, and either wait 30 minutes or use a different phone line to speak to Amazon customer services. You can find more information about Amazon scams on their help pages, by .

You can read more about the scam here: Woman warns of new Amazon scam seeking account details.

Car Insurance Scam

Ghost broking is a term you may not have heard before, but it's thought up to 21,000 people in the UK have fallen victim to a car insurance scam. Last year, 517 reports were made by victims, according to Action Fraud. The Insurance Fraud Bureau says insurers last year collectively reported more than 21,000 policies that could be connected to the scam.

Ghost brokers can be individuals or groups that are unlicensed, who pose as middlemen for insurance companies and claim to be able to find cheap car insurance prices for those struggling to get affordable cover. This can include selling bogus paperwork to victims, and they'll often sell a policy that will appear against the vehicle on the Motor Insurance Database (MID). Ghost Brokers often advertise on student websites or through WhatsApp and social media.

However, while the deal may initially look good, the Ghost Broker may then cancel the policy without the purchaser knowing a couple of weeks later, so the Broker then gets the money back. The purchaser then becomes a victim of fraud as they will be without insurance, leaving them open to be liable for fraud and at risk of penalties for driving uninsured.

In 2021, ghost broking victims who contacted Action Fraud reported losses of £1,950 each, on average.

How to avoid falling victim to a Ghost broking Scam:

- Look for proper contact details with any advertisement- not just a phone number or email address.
- Check the Financial Conduct Authority's (FCA) website for a list of authorised brokers.
- If they are not listed - stay away.
- Get in touch with the insurance company the cover is with- check the cover directly with them.

Cyber Security

The Internet of Things

We are all surrounded by technology these days, with smart devices playing a growing role in our own homes. Smart devices include things like smart speakers, video doorbells, wi-fi controlled electricity sockets, home security webcams, smart fridges, and even wi-fi enabled light bulbs. In Cyber Security circles, these devices are also described as the “internet of things”, referring to the way that the products are connected within our homes (usually via our home wi-fi).

Smart devices aim to make every day life easier and more convenient. However, having all of these devices around us also means that there are more potential targets for cyber criminals to try to compromise. All of these devices can be hacked, and could offer criminals a route into your home wi-fi network.

The good news is that with a bit of know-how, you can set these products up safely.

Firstly, you should make sure to set up your new device following the instructions from the manufacturer. If you try to set the device up intuitively, you might miss important steps which impact on the device’s security.

Some smart devices require you to download an app to be able to interact with your smart device. If you need to use an app, have a look at the security and privacy settings within the app to see if you can switch on Multi Factor Authentication. If it's available, it's always worth activating. Multi Factor Authentication will protect your account if your password is compromised, as the criminals won't be able to get into your account without providing a second form of proof of identity (such as a unique one-time pass code which is sent to you via text, or by using your fingerprint to authorise the log in).

You should make sure you set up your user account for your device using a strong, unique password. That way, if your password is leaked, the criminals will not be able to get into any of your other accounts.

Some devices come with a default password that you will be expected to change (such as "0000" or "admin"). These default passwords are easily guessed, so it is important that you change the default password as soon as possible.

It is also important to make sure you keep your devices updated. You can keep on top of this by switching on the option for installing automatic updates for each device, and accepting manual updates when they appear. Finally, if you decide to sell or give away your device, perform a factory reset before handing it over. You can find more information on this topic on the National Cyber Security Centre website.

Advice for Staff

Secondary Employment Best Practice

The Covid-19 Pandemic has irrevocably changed working practices across all sectors of the NHS. This progression was in many cases long overdue and working from home options combined with on-site working are now considered part and parcel of working life for many - both in the NHS and elsewhere across all employment sectors.

With the current economic crisis escalating the cost of living, it's understood that wages are not going as far as before. This has led some to seek a second job or to pick up non-contracted work outside of their contracted hours- as they are perfectly entitled to do.

Staff are, however, urged to declare any secondary employment to their line manager and seek approval if needed. This may well even be a contract requirement- check with your line manager if you are unsure. Counter Fraud strongly advise against taking on any extracurricular work that overlaps current contracted hours or that impacts negatively on any staff member's main job role.

Staff are reminded that calling in sick and working elsewhere during the declared period of sickness could amount to fraud and may lead to prosecution, or disciplinary action at the very least. While offers from agencies for work at well above the normal market rate may be tempting, any shifts agreed or taken on and worked must be outside of regular contracted hours.

Staff who are in the position to be working from home are urged to work only their contracted role during their contracted hours. If the economic climate is leading any staff to pick up secondary employment, this must be outside of contracted hours, without any overlap and MUST be declared and documented as per the relevant organisation/department procedure.

If in doubt, staff are advised to speak with their line manager in the first instance. Don't fall foul of crossing the line of what is acceptable and what isn't- knowingly or otherwise. If in doubt, always seek advice.

In the Press

Jail Sentence for Banker who Faked Consultant Documentation

Rajesh Ghedia, a former banker, has been jailed after it emerged that he had committed fraud. Ghedia had forged documentation which he claimed was from a Consultant at a private practice in London. He used the fake letters to commit a £1.2 million insurance scam, claiming that he had a terminal illness. Ghedia also convinced acquaintances and family members to invest in a fake Goldman Sachs portfolio.

In total, Ghedia made £1.8 million from his actions, which involved 30 separate fraud offences. He has now been sentenced to 6 years and 9 months in prison. A Proceeds of Crime Act application will now be made in order to recover the money lost by his victims. You can read more about the story here.

11 year sentence for Green Investment Fraudsters

The Serious Fraud Office (SFO) have secured the conviction of two fraudsters who scammed 2,000 investors out of their savings and pensions. Andrew Skeene and Junie Bowers misled potential investors into thinking that their money would be investing in an ethical scheme which would protect the Brazilian rainforest whilst supporting local communities. In reality, the money was used by Skeene and Bowers to fund their own lavish lifestyles. Over £2 million was spent on retail, whilst Skeene used the investment fund to pay for his wedding, and Bowers bought himself a Bentley Continental GT. Some of their victims had been unable to retire as a result of losing their life savings and pension pots.

Skeene and Bowers had scammed investors out of over £37 million. The pair have been sentenced to 11 years in prison and have been disqualified from acting as directors for 10 years. You can read more on the SFO website.

Counter Fraud Training

Open offer for bespoke training/fraud awareness input

The counter fraud team is always happy to put together bespoke training for your specific role or department. We are also happy to attend any team meetings to introduce ourselves and talk about NHS Fraud.

If you would like to arrange a session for your team, please contact one of the Local Counter Fraud Specialists.

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. 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.