Counter Fraud Newsletter February 2024

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

NHS Staff Security Awareness - Tailgating

Although security matters are not always fraud related, weaknesses in physical security arrangements can lead to fraud being committed against organisations and individuals. A good example is where criminals 'tailgate' or follow staff into NHS premises, often aiming for restricted or controlled areas.

Once inside they engage in theft or use information gathered to commit fraud. This is why it is so important that staff are aware of suspicious people trying to access NHS buildings and restricted areas. Some signs to be aware of are:

- Individuals loitering by entrances or attempting to follow staff as they enter.
- Using pleasantries or engaging in conversation to distract the member of staff so they don't realise the imposter isn't meant to be there.
- Use of props to lend an air of false authenticity or authority – such as lanyards, fake ID badges, hi-viz jackets or clipboards etc.

Staff should challenge anyone who they are concerned about, if they are confident to do so, or otherwise call security immediately. Genuine staff, contractors and visitors will not mind being asked the purpose of their visit and directed to the correct access point / reception.

Once a criminal or imposter is inside NHS premises there is a risk of theft of staff belongings, NHS property, controlled drugs and other potentially harmful substances. Criminals may also aim to harvest information that can assist them to commit fraud at a later point – this could be staff personal information, bank cards, passwords, PIN numbers etc. Laptops and PCs which are left unlocked can also be a source of confidential information that could be used for criminal purposes.

In some cases organised crime groups have used tailgating to target NHS staff – a group called the 'Coventry Falcons' would follow hospital staff into secure areas whilst wearing clinical uniforms. Once inside they would steal bank cards and use information gathered during their unauthorised visit to trick their victims into believing they were their genuine bank calling them. This led the victims to give away their PIN numbers – resulting in big losses to some individuals.

The Coventry Falcons were stopped and the ringleaders jailed, but this crime model is still used and staff should always be vigilant and maintain awareness – don't allow Tailgaters access or you could be the victim

Current Scam Trends

Bank Impersonation Scams

After a recent fraud committed over the phone where the fraudsters impersonated officials from the victims' banks, Ofcom has warned against relying on caller ID to tell if calls are legitimate.

A scam tactic called "spoofing" allows fraudsters to disguise themselves with the phone numbers of legitimate organisations like banks. When the call arrives on your phone, the fraudsters real phone number is hidden, and they can choose what number flashes up on your screen.

Combined with social engineering tactics such as the caller using a professional script, knowing details of your bank account, and even warning you against the risk of scams, fraudsters can make themselves sound genuine.

Communications regulator Ofcom has advised: "Never give out your personal information in response to an incoming call, or rely upon the caller ID as the sole means of identification, particularly if the caller asks you to carry out an action which might have financial consequences."

It is not just banks' phone numbers that are spoofed. There have been instances with fraudsters claiming to be from Amazon, energy companies, and service providers such as Microsoft. There have also been phone calls purporting to be from a GP, or from a local pharmacy, asking for that victim to provide bank details so that they can pay for their prescriptions or pay for a delivery service (see last month's newsletter for more about this scam).

If you receive a call claiming that something is wrong with an account or service, or asking for personal / financial information, hang up and call the provider using a known phone number. It is important to either wait half an hour or use a different phone to make the call as the fraudsters can jam your line and intercept outgoing calls. You can report suspicious phone calls to Action Fraud by phone (0300 123 20 40) or using their online reporting tool.

Recruitment Scams

Fraudsters are taking advantage of the competitive job market to exploit unsuspecting job seekers. These types of scams have become more sophisticated and in some instances, victims have even attended job interviews for posts that do not exist. Some of these recruitment scams, like the one in this BBC news article, start via WhatsApp or text.

Recruitment Fraud Red Flags

- **Unrealistic offers**: Scammers often lure victims with promises of high salaries, minimal working hours, and extravagant perks.
- **Unsolicited Job Offers:** Be cautious if you receive job offers out of the blue, especially if you have not applied for the position. Legitimate employers typically follow a formal hiring process.
- **Vague Job Descriptions:** Watch out for job postings with unclear responsibilities, requirements, or company information. Legitimate employers provide comprehensive details to attract qualified candidates.
- **Upfront Payments:** Scammers often request payment for background checks, training materials, or other dubious reasons. Legitimate employers often cover these costs themselves or recover costs from your first salary payment.

Protecting Yourself

- **Research the Company:** Legitimate organisations have an established online presence, including a professional website and active social media profiles.
- **Verify Contact Information:** Confirm the company's contact details, such as their phone number and email address.
- **Check Online Reviews**: A lack of online presence or overwhelmingly negative reviews can be red flags.
- **Use Reputable Job Platforms:** Verify the legitimacy of any platform before submitting personal information.
- **Be Wary of WhatsApp Communications:** Legitimate employers typically use official email addresses and phone numbers.
- **Protect Personal Information:** Don't share your bank details during the recruitment process. Legitimate employers typically request such information after a job has been offered and you begin your post.

Cyber Security

Focus on Romance Scams

It's not just your heart on the line...

Lloyd's bank have recently published data reporting that there was a 22% increase in romance fraud during 2023.Romance fraud is a particularly damaging type of scam. All fraud involves a degree of manipulation or deception, but romance fraudsters aim straight for your heart.

Their goal is to hook unsuspecting victims by building a one-sided but intense emotional connection, before persuading the victim to send them money. The fraudster will often claim that they have had a personal emergency - perhaps they're abroad and their cards have stopped working, or they've had to access urgent medical care and there's been a problem with their travel insurance.

These fraudsters rarely ask for money straight away. Usually they will spend days, weeks or even months, building a rapport and a false sense of trust. They will always have an excuse why they cannot meet up or video call, and often use someone else's photographs and / or identity to appear legitimate. Sometimes they will even impersonate well known public figures - actors such as Keanu Reeves, Jason Statham and Liam Neeson have all been impersonated.

We might think we would never fall for this type of scam, however, it is difficult to see clearly when you're in the grip of a professional manipulator. A recent article in the Guardian by Becky Holmes (who has fun frustrating would-be-romance-scammers) highlights that people from all walks of life can be taken in by these scams. She interviewed a doctor, a chief executive, a lawyer and a detective who had all been victims of the romance fraud methodology.

Some Signs of a Romance Scam

- **"Love bombing"** - They bombard you with highly emotional messages, praise and affection in an attempt to get your trust.
- **Requests to move conversations away from where you met them.** They will want to come away from dating sites / social media quickly in case their dodgy profile is reported by a different victim.
- **Their profile photo is from someone else's account.** If you do a reverse image search, you can see if a photo is being used somewhere else. Some real people have had their photos and personal details used thousands of times by scammers.
- **A fantastical back story.** These scammers often claim to be famous, or very high achievers in the army or medicine.
- **A sob story.** Before too long an emergency will come up such as a medical crisis, lost wallet, or missing salary payment. Requests may start small and they always promise they will pay you back.

How to Reverse Image Search

There are a few different ways to reverse image search. The easiest is to save a copy of the photo you want to check onto your device.

Then, open Google, and instead of typing into the search box, click the small camera icon on the right. Upload the image you wish to search for, and Google will do the rest.

They will show you any exact matches, as well as similar images. Please note, if an image search doesn't bring back any results, this isn't proof that the person is genuine. Listen to your gut, and if you are in doubt, seek advice.

Protecting Yourself from Romance Scams

- Do not share your personal information online.
- Do not send money to someone you've never met.
- Be wary of moving conversations off official platforms.

- Trust your gut - if something feels off, it probably is.
- Speak to friends and family - it's often easier for them to see things objectively as they're not on the receiving end of any emotional manipulation.
- Notify your bank immediately if you think you've been tricked into making a payment to a fraudster.

Who Commits Fraud?

In short, anyone can commit fraud. It is not a violent crime and given a set of circumstances, anyone could be tempted.

Criminologist Donald Cressey determined that three factors were needed in order to commit fraud:

- **Pressure –** the person committing fraud may be in debt, or they may want a lifestyle that they would struggle to fund legally.
- **Opportunity** – This is usually a weakness in procedures which allows a fraud to take place. Technology provides many opportunities for fraudsters to take advantage.
- **Rationalisation** – The person justifies why it's ok to commit fraud. In the case of the NHS, some people will see a bottomless pit of money with no victim's face attached and will tell themselves that it's ok to take a little extra.

Delving a little further into why people commit fraud, the Commonwealth Fraud Prevention Centre in Australia have defined 8 different personality traits, or persona, of fraudsters:

1. **The Reckless.** This criminal is thinking of themselves and has no regard to their actions and the consequences. An example of this could be a contractor bidding for a contract they do not have the means to fulfil. They then have to compromise their work or lie about what they have done resulting in payment being made which was not earned.

2. **The Exploiter.** Somebody who takes advantage of something they have access to, in a harmful way. A patient who has access to a stash of blank appointment cards uses them to claim for appointments they did not have in order to receive travel compensation.

3. **The Impersonator.** Somebody who uses a fake identity. For example, a person could legitimately register at an agency to do bank shifts. They book the shifts but the person who turns up to do the shift is not the person who booked it and has been through the appropriate pre-employment checks. The person turning up may be in the country illegally or may not be qualified to register themselves at the agency.

4. **The Fabricator.** Somebody who creates false documents to receive something. It could be somebody producing fake ID to gain employment, a staff member producing a made up expenses receipt or a patient creating a false prescription to name but a few.

5. **The Coercer**. These people manipulate somebody to do something they shouldn't. This could be through threats, bribes or social engineering. Sending a phishing email to dupe a staff member to reveal their log in details could be seen as coercion.

6. **The Deceiver.** This fraudster will make deliberate false statements or withhold something they should declare. An example of this is somebody who does not declare that they have a criminal conviction on a job application in order to receive a job offer.

7. **The Concealer.** Somebody who hides their activity. For example a staff member who has secondary employment may hide this in order to work simultaneously or during a period of sickness to receive more pay.

8. **The Organised.** Organised crime groups pose a huge threat with targeted and planned attacks. They are behind many of the phone and email scams we see.

Fraud is a complex crime which can be committed by people who would not consider breaking the law in any other way. Being mindful of how and why people commit fraud will help to recognise when something may not be quite right.

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: