Counter Fraud Newsletter October 2023

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

Fighting Fraud Together

In today's digital world, fraud has become more advanced. Cyber-criminals are constantly creating new ways of trying to trick people. However, all of us can play a vital role in preventing fraud.

- **Education Is Your Shield**: Staying informed about the latest scams is your first line of defence. The more you know about how fraudsters behave and what their current strategies are, the better your chances of spotting scams in the wild.

- **Scepticism: Your Inner Lie Detector**: When you encounter suspicious emails, adverts, text messages or other offers that seem too good to be true, being sceptical can save you from trouble. Always take the time to consider what steps you can take to check if something is legitimate. There's loads of advice available online covering loads of different scam types (e.g. search "romance scam advice" or " Facebook marketplace scam advice" to see some examples).

- **Listen to Your Gut (Intuition)**: If something feels off, take a moment to pause and think. This piece of advice is central to the fraud awareness campaign run by Take 5 to Stop Fraud, as fraudsters will often try to panic you or rush you into making a mistake.

- **Speak Up and Report**: Talking about fraud and reporting it can help prevent others from falling into the same traps. It also exposes the tactics fraudsters use. You'll find advice on how to report different types of fraud on page 5 of this newsletter.

In our interconnected world, people armed with knowledge, skepticism, intuition, and open communication are the front line of defence against fraud. Together, we can outsmart the fraudsters and keep ourselves and others safe.

Current Scam Trends

Property to Rent Scams

Fraudsters have been taking advantage of the shortage of rental properties, rising rent prices, and high levels of demand. Usually, these scams start with a post on social media advertising a property or room to rent at an attractive rate.

In some of these scams, the fraudster asks the victim to pay a deposit or rent in advance, before the victim has been able to view the property. Once paid, the fraudster cuts all contact.

In other cases, victims have been shown around properties, asked to sign official-looking contracts, and have even been given keys after paying a deposit. However, when they later try to move in they find their key doesn't work and / or that there is someone else already living at the address. The "landlord" vanishes, leaving the victim out of pocket.

Advice

- Be wary of accommodation advertised on social media or unregulated platforms. Photos can be stolen from genuine listings.

- All letting agents and property managers must be registered with a government-approved redress scheme. The National Trading Standards website has a tool where this can be checked.

- Look out for pressure tactics - if the “landlord” is trying to panic you into sending money, take a step back.

- There is more advice on how to keep yourself safe from these scams on the Which? website.

Vehicle Tax Scams

The DVLA now allow you to set up tax and MOT reminders via text or email. This is excellent news for fraudsters.

Pesky criminals are trying to lure motorists into a trap by saying that they are owed a refund. Others threaten you with a fine if you don’t make a payment, or tell you that your payment has failed and you are driving round illegally.

The DVLA have confirmed that they will never contact you via email or text asking you for either your personal details or payment information.

Advice

- You can check your car tax and MOT status by visiting the official DVLA website

- Make a note of your renewal dates on an electric calendar or in a good old fashioned paper diary.

- Avoid posts on social media which show your car registration or any driving documents

- If are in a car lease scheme, check what is included. You may not be responsible for arranging the tax on the vehicle you have.

Crypto Investment Scams

As the cost of living continues to bite, crypto-currency investment schemes can seem tempting. Adverts often pop up on social media, and you may even see that a friend or celebrity appears to be endorsing a particular scheme.

However, there are huge numbers of crypto currency scams going round. The fraudsters behind these scams go to significant lengths to carry out their attacks. This includes creating websites, investment “dashboards”, customer portals, reports on returns, and even fake policy and procedure documents.

Fraudsters also promote these schemes using deep-fake technology and hijacked social media accounts, giving the impression that people you trust are endorsing them. Victims of crypto-currency investment scams come from all walks of life, including experienced finance professionals, which shows just how convincing these scams can be.

Advice

The Natwest website has some really helpful advice on protecting yourself from these scams.

- **Take your time -** be wary of pressure tactics such as pushy / persistent phone calls and time limited “trading events”.

- **Be sceptical of social media adverts -** the scammers may use unauthorised or fake photos / videos, or hijacked social media accounts to claim that a trusted party has endorsed them.

- **Seek advice -** speak to a reputable source before making any investments.

- **Registration -** Ensure any financial firms you deal with are on the FCA register.

Cyber Security

Remote Access Scams

Remote Access Frauds are on the rise nationally with a variety of methods being reported.

Usually, the victim is contacted by telephone and the caller might claim they've spotted a problem with the victim's computer and offer to take remote control of the device to fix it.

They may even say they're calling from the victim's bank and need to help with a problem with their account.

- They will then convince the victim to install a piece of software that enables them to have remote access to their computer.

- During the call, the victim will be instructed to login to their online banking. Remote access software is used to blur the victim's screen whilst the scammer makes fraudulent transactions from the victim's account.

- The victim may be asked to read out a series of numbers the scammer claims they have sent to the victim's mobile. In reality, these numbers will be one-time verification codes from the victim's bank which will allow the fraudster to bypass security controls to transfer money out of the victim's bank account.

Some victims have reported slightly different versions of how the scam is perpetrated. However, the goal and general methodology of the fraudsters remains the same.

Advice

- Never install any remote access software on your device as a result of an unsolicited telephone call, browser pop up, or text message.

- One-time verification codes sent to you by your bank to authorise transactions on your account should never be shared with anyone, not even bank employees.

- If you believe your laptop, PC, tablet or phone has been infected with a virus or some other type of malware, follow the National Cyber Security Centre's guidance on recovering an infected device.

- Protect your money by contacting your bank immediately on a different device from the one the scammer contacted you on.

- Make sure your computer is protected with regularly updated anti-virus and anti-spyware software, and a good firewall.

Cyber Security Awareness Month 2023

October marks Cyber Security Awareness Month, a global initiative aimed at raising awareness about the importance of cybersecurity. The NHS holds a huge amount of sensitive data, ranging from patient records to operational and financial information. Unfortunately, this makes the NHS a prime target for cyberattacks. Here are some key measures we can all take:

Phishing Attacks: Be cautious when opening emails, particularly those requesting personal details or containing dubious links or attachments.

Robust Passwords: Use strong, unique passwords for your accounts. Use passwords that encompass a combination of letters, numbers, and symbols or use the three random words method.

Two-Factor Authentication (2FA): Activate 2FA wherever you can. This additional layer of security can help thwart unauthorised access attempts.

Routine Software Updates: Keep your devices and software up to date to reduce the risk of exploitation.

Report Suspicious Activity: Promptly report concerns to your IT department and speak to your Local Counter Fraud Specialist.

Secure Remote Work: When working from home, use VPNs and follow the same cybersecurity protocols as you would in the office.

Policies and Procedures: Follow your organisation's policies and procedures when handling and safeguarding sensitive information.

Continuous Learning: Cyber-criminal's tactics are constantly evolving. Make sure to read our monthly Counter Fraud newsletter and sign up to our Cyber Fraud Masterclasses.

This Cyber Security Awareness Month, remember that we all have a vital role to play in protecting the NHS.

For further information, please see the NHS Digital Website: Cyber Security Awareness Month.

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: