Fraud Counts Newsletter

International Fraud Awareness Week 2023 – Edition 2

Introduction

Welcome to our latest edition of our Counter Fraud Newsletter for NHS staff.

This newsletter contains information on how you can help in the fight against fraud, current scam trends including Social Media Hijackers, Fake Customer Service Accounts on X (formerly known as Twitter), Cyber Remote-Access fraud, a reminder on reporting fraud concerns, and how to contact your Local Counter Fraud Specialist.

Fighting Fraud Together

It's true what they say... prevention *is* better than cure!

One Hundred and Twenty-Three and counting...

We're all becoming more and more aware of fraud as a big problem. Most of us will know of someone who has fallen foul to a scam or been contacted in an attempt. We've probably all received fake emails or text messages, phishing attempts designed to make us panic that we haven't done or need to do something to safeguard ourselves against a loss or some further action.

But... do we take what we know about fraud in our personal lives into our work lives and use the same knowledge and skills to help prevent fraud within the NHS?

40%

It's very important to be aware of fraud in this digital age where **more than 40% of all crime is now fraud** and crime of this type is most easily perpetrated via digital means.

Take a couple of moments to consider how the NHS might be a victim of fraud. If you need some help, visit the NHS Counter Fraud Authority's website and browse through the information.

Recent work in this area has highlighted 123 ways in which the NHS might become a victim of fraud. As you'd expect, these range in severity and potential levels of loss but each and every one of them presents an opportunity for a fraudster and poses a risk to our NHS.

Everything we do to prevent or deter fraud in the NHS helps, no matter how small or how big that thing might be.

©ASW Assurance

Prevention Advice – Know Your Stuff

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

- Fraudster's tactics are constantly evolving. Make sure to read our Counter Fraud newsletter to keep up to date

It's Who You Know

- Know who to contact to report a suspicion or discuss a concern and don't be shy about speaking up.



Be Fraud Aware *EVERYWHERE*: Don't get caught out at work or at home.

©ASW Assurance

Current Scam Trends

Social Media Hijackers

A recent article on the This is Money site highlighted a social media scam exploiting people's trust in small businesses.

The scammers targeted Julie Ashworth, who runs as successful business mostly via Instagram. They convinced her that she needed to "secure her account" and tricked her into sharing her log in details.

They locked her out of her account and messaged her customers using her profile. They told her followers they were at risk of being hacked too and directed them to follow the same process that had been used to steal her account. Similar tactics are used to encourage social media users to engage in fake investment scams, taking advantage of people's increased trust in figures they follow or engage with on these platforms.

Prevention Advice

- Protect social media accounts with strong, unique passwords.
- Where it is available, turn on Multi Factor / Two Step Authentication. This option is usually found in the Security or Privacy section of the app settings.
- Be wary of emails or direct messages claiming you are at risk and need to click on links or follow instructions. Watch out for fake investment scams or requests for money or your personal / sensitive information.

Fake Customer Service Accounts on X (formerly known as Twitter)

The Guardian has reported that customers using X (formerly known as Twitter) to contact companies to raise complaints or request refunds are being targeted by fake "verified" accounts.

On the X platform, users can pay £11 a month to have a blue "verified" tick added to their profile. Some fraudsters are exploiting this option, setting up profiles designed to look like they belong to a verified member of the company's customer services team. Having a blue tick makes the profiles look more convincing.

The fraudsters use these profiles to contact people who are seeking assistance - such as those who have lost out due to flight cancellations and delays. You can read more on the Guardian website.

Prevention Advice

If you contact a company on social media, be aware that responses may be from fraudsters.

Look closely at the details. Giveaway signs of a fake customer services account can include:

- Small changes to the usual format of the account name (such as unexpected hyphens)
- The account has only been registered for a short time.
- The fraudster tries to move you onto a different platform (e.g. WhatsApp).

If you're in any doubt, use an alternative and official route to contact the company.

©ASW Assurance

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.

Prevention 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.



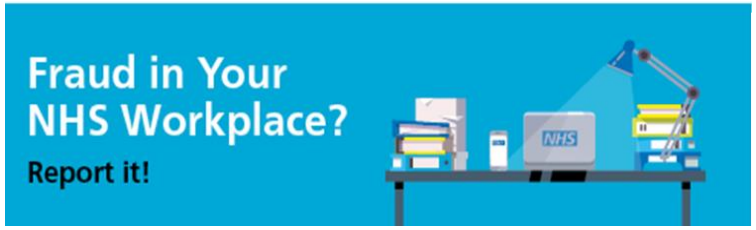
Suspicions of Fraud and Bribery may be reported anonymously by telephoning the NHS Reporting Line in confidence – 0800 028 40 60 or www.reportnhsfraud.nhs.uk



©ASW Assurance

A Quick Guide to Reporting Fraud Concerns

I have a concern that fraud may be being committed against the NHS.	You can contact your local Counter Fraud team using the details overleaf. 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 team for advice and support using the details overleaf.



If you have any suspicions or concerns,
You can call us anonymously on

0800 028 40 60

POWERED BY **CRIMESTOPPERS**

Or search 'NHS Fraud' online for more information

The NHS Counter Fraud Authority leads on fighting fraud, bribery and corruption in the NHS and the wider health group

NHS Counter Fraud Authority

Department of Health & Social Care

©ASW Assurance

Our Local Counter Fraud Team

Our Local Counter Fraud Specialists are fully accredited with the University of Portsmouth. We aim to prevent and deter fraud and hold those to account who commit fraud against the NHS. Counter Fraud Services are provided by ASW Assurance (www.aswassurance.co.uk), an NHS consortium providing counter fraud and internal audit services to NHS and healthcare organisations.

If you would like to know more about our Counter Fraud work or arrange for your department to receive a Fraud Awareness Presentation, please contact one of our team below.



Gareth Cottrell – Counter Fraud Manager

✉ gareth.cottrell@nhs.net ☎ 01872 258057
07814 002364



Tracy Wheeler – LCFS

✉ tracy.wheeler2@nhs.net ☎ 01752 431378
07789 868568



Byron Kevern – LCFS

✉ byron.kevern@nhs.net ☎ 07775 417508



Sarah Smith – LCFS

✉ Sarah.Smith10@uhbw.nhs.uk ☎ 07467 685609



Sandra Bell – LCFS

✉ sandra.bell19@nhs.net ☎ 07467 685529



Ian Halkerd – LCFS

✉ ian.halkerd@uhbw.nhs.net ☎ 07788 300215



Sammy Donaldson – Trainee LCFS

✉ s.donaldson1@nhs.net ☎ 07467 685529