Fraud Counts Newsletter

Spring 2023 – part 2

Introduction

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

This newsletter contains information on current scam trends including WhatsApp code scam, tab napping, Eurovision phishing, holiday scams, cyber security, fraud cases currently in the press, a reminder on reporting fraud concerns, and how to contact your Local Counter Fraud Specialist.

Current Scam Trends

WhatsApp code scam



Fraudsters have been targeting WhatsApp users by posing as a friend and asking for a security code. The scam begins when a criminal gets access to another WhatsApp account which has you listed as a contact. The fraudster, posing as your friend or someone that's a member of a WhatsApp group you're in, will then send you seemingly normal messages to try and start a conversation with you.

However, around the same time you will receive a text message from WhatsApp with a six-digit code. This is because the criminal has been trying to login to WhatsApp using your mobile number.

The criminal will claim that they sent you their code by accident and ask you to help them by sending it to them. Once the fraudster has this code, they can login to your WhatsApp account and lock you out.

The criminal will then use the same tactic with your WhatsApp contacts in an effort to steal more accounts and use them to perpetrate fraud.

What you need to do

- If you are willing to do so, set up two-step verification to give an extra layer of protection to your account: Open WhatsApp and tap the 3 dots in the top right corner of your screen > Settings > Account >Two-step verification > Enable.
- THINK. CALL. If a family member or friend makes an unusual request on WhatsApp, always call the person to confirm their identity.
- Never share your account's activation code (that's the six-digit code you receive via SMS).
- You can report spam messages or block a sender within WhatsApp. Press and hold on the message bubble, select 'Report' and then follow the instructions.

©ASW Assurance

Tab napping
This odd term is a type of phishing attack which can happen if you have several tabs open at once on your computer or laptop.

A 'same-origin policy' is a security feature which isolates websites from each other. The same-origin policy does have some 'holes' which websites use when interaction is necessary. It is through these holes which tab napping can occur.

Hackers can use JavaScript to change the content of an open but inactive tab. Changes will usually be made to look like a default log in for your bank, emails or social media account.

When the user goes back to the tab, the hacker is hoping that they will assume they have been timed out and will put their log in details again. If the user logs in again, the hacker can harvest the details and use them to commit other offences, with the user being the victim.

Top tips to prevent tab nabbing:

- Close down a tab when you are finished with it and open a new one when you need it again instead of keeping lots of tabs open.
- If you do keep tabs open, have a system which means that you can spot if something changes. For example, always have tab 1 open for emails, tab 2 for an intranet and tab 3 for all other browsing.
- If the site you regularly visit looks different, such as an unusual layout or spelling errors, be suspicious.
- Check that the URL shows a secure protocol, such as HTTPS.
- Keep anti-virus and spyware up to date.

Eurovision phishing
Cyber criminals are targeting hotels hosting people travelling to Liverpool for the Eurovision song contest event in May 2023.

The online travel agent booking.com told the BBC they have seen evidence of "some accommodation partners being targeted by phishing emails."

Cyber criminals take advantage of news and current events to scam customers. The usual advice applies if you believe you have become a victim: report to Action Fraud, relevant bank or credit card companies and/or your insurer.



Holiday scams
Many of us will be looking forward to the summer, planning days out and holidays. Please be aware that fraudsters will post fake holiday adverts and event tickets online. This is particularly a risk on social media where accounts are easily hijacked, created and deleted.

Remember - if it looks too good to be true, then it probably is.

You can find some really useful advice on Holiday Scams on the Which? website.

©ASW Assurance

Cyber Security



Artificial Intelligence – Future Fraudster?

Artificial Intelligence (AI) has the potential to make life easier – indeed many of us already use AI in our daily lives. It pops up all the time - whether it's a smart speaker telling you the weather forecast, Maps letting you know that there's heavy traffic building up on your planned route, or Spotify compiling the ultimate playlist to transport you to your teenage years, AI is already embedded in our home and work environments.

Unfortunately, the development of more sophisticated AI tools, such as Chat GPT, brings with it many new fraud risks. Chat GPT generates text at the request of the user – and what makes it unique is that it produces text with a “human tone”. This makes it much harder to tell that the content has been produced by a machine.

At work you will almost certainly have received phishing emails that have been produced by a fraudster. Traditionally, these scam emails have had tell-tale warning signs, such as strange wording, or spelling and grammar errors that help us to spot them.

AI can create convincing phishing emails as it is unlikely to contain spelling or grammar errors, and it has been designed to sound "human". There is also new AI powered voice generating software, which can allow a fraudster to "hijack" your voice using a 3 second clip of you speaking.

Alongside these developments, there has been a rapid growth in AI art generators. These have become very popular as the user can generate impressive, bespoke profile pictures/content for use on social media. Unfortunately, some of these apps have hidden viruses lurking behind the scenes which can compromise your device and data. You may also come across AI-enabled scams on social media sites, such as this one which was spotted on Linked In recently.

Keeping yourself safe

Always be suspicious if you are asked to click on a link in an email or on a social media post.

If you are on a desktop or laptop, you can use your mouse to hover over the link to see where it will take you.

It is not easy to hover over links on touch screen devices. If in doubt, log into a desktop/laptop and hover over the link.

Be wary about which apps you download – you can find some useful advice on safe app interaction on the Verified website.

©ASW Assurance

In the Press



Guilty verdicts after fraud investigation uncovers bribery issues at NHS Trust

Two men have been found guilty of fraud and bribery offences against the NHS. A third man entered a guilty plea ahead of the seven-week trial. The court heard that Hasan Abusheikha, a Theatre Manager at St Albans City Hospital Trust, had used his position to secure bribes from Elmo Emanuel, the CEO of Implants International and Xtremity Solutions Ltd. Another supplier, Jawid Khan of TSI Med Ltd. entered a guilty plea before the trial began.

It was found that Abusheikha had accepted bribes from Emanuel and Khan in exchange for making sure that the Trust procured medical equipment from their companies. Abusheikha was also convicted of accepting payments from two other suppliers. The total value of the offences was assessed as being more than £600,000.

All three men will be sentenced at St Albans Crown Court. The NHS Counter Fraud Authority and the Crown Prosecution Service will launch proceedings to try and recover money taken from the NHS. You can read more on the NHS Counter Fraud Authority website and on the BBC news website.

Three arrests in Personal Protective Equipment (PPE) fraud case

Three people have been arrested following a National Crime Agency investigation into international PPE fraud. A husband and wife are amongst those arrested. The male is suspected of setting up a UK company in order to run a PPE scam during 2020 which was global shortages in supplies of safety equipment. His wife is suspected of helping him to launder the proceeds.

The investigators believe the company agreed sales of PPE with a total of over $35 million to customers in the USA and Germany. Customers were told to pay an upfront fee to secure their order. They were informed that the fee would only be released once the contract conditions had been met. However, the company owners could access the account without delivering the goods agreed. The case is still open and the suspects are being interviewed. You can read more about this case on the National Crime Agency website.

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

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.smith337@nhs.net ☎ 07467 685609

©ASW Assurance