COVID-19 Fraud & Security Alerts

December 2020

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

Cyber criminals know that the NHS is busy

Attacks against the NHS continue, as online criminals seek to exploit patients, staff and health systems at a time of national crisis.

Techniques seen recently have included bogus emails with links claiming to have important updates which, once clicked on, lead to devices being infected. Cyber criminals pose as people they're not, such as staff within government organisations, banks and suppliers. Attacks also take place as phone calls.

Although the National Cyber Security Centre has taken measures to automatically discover and remove malicious sites which push phishing and malware, the current level of attacks will have a more damaging impact since the NHS has less capacity to respond quickly to mitigate the damage.

With the increasing stress on the NHS, especially those at the front line of the fight against Covid-19, there is an even greater imperative that existing protocols are adhered to. Any attempts to circumvent the normal rules and procedures could leave an organisation wide open to cyber criminals and others to take advantage and have a catastrophic effect.

It is important that everyone is extra vigilant and individual users are aware that SPAM emails and scam phone calls are on the increase.

To avoid systems becoming infected or individuals and organisations compromised colleagues should:

1. **Be vigilant and suspicious** – if something looks too good to be true it generally is. If an email comes from a colleague but doesn't sound like them and isn't formatted in the way they would write – be suspicious. Call your colleague to check.
2. **Never give out your own or anyone else's passwords, bank details or other sensitive data**. A legitimate organisation will NEVER ask for this data via email (or telephone). If in any doubt don't say anything and seek advice. It is best to be cautious.
3. **Check links in any password reset (or other) emails very carefully** – check they are taking you to a legitimate site. If in doubt, navigate to the site directly (without using the email link) and login directly. This is a common "phishing" technique.
4. **Don't open attachments** from anyone you don't know or that are not from a trusted source.
5. Don't reply to spam or forward chain emails.
6. **Change your passwords regularly** and do not use the same password for all accounts, both at home or at work.
7. **Do not** unsubscribe from any unsolicited "spam" emails – this just confirms you are a real address.

The National Cyber Security Centre website has lots of useful information and links on how to protect your personal information. Organisations are also being urged to follow cyber security best practice as they continue to support home and remote working as part of their response to COVID-19. Their advice here provides tips for staff using laptops, mobiles and tablets to help spot typical signs of phishing scams.

Staff are advised to report any concerns to their IT service provider.

NHS Counter Fraud Authority annual report and accounts 2019 to 2020

The NHS Counter Fraud Authority is responsible for putting in place an NHS-wide counter fraud strategy. It has recently published its latest annual report and account. To access the report please click here.

NHS scammed: Cyber-gang trick NHS into sending £1million to their bank accounts

The Sun has recently reported that a cyber-gang has targeted the NHS, by contacting accounts staff and getting them to substitute their bank details for those of the real suppliers. Investigators stated that they have uncovered sophisticated mandate fraud at one NHS body. This has led to 11 people being arrested and 16 people being interviewed under caution. The activity was revealed in the annual accounts of the NHS Counter Fraud Authority.

Read the full article here

Warning over coronavirus vaccine text message scam

People are being warned not to fall for fake text messages that claim to be from the NHS offering the coronavirus Covid-19 vaccine. Health trusts and the Government's National Cyber Security Centre have issued warnings about the text messages. The texts offers the vaccine, pretending to be from the NHS or your local doctor's surgery, but are fake and the link it invites you to click takes you to a fraudulent website. NHS trusts and GP surgeries across the country have issued warnings about the scam, as well as advice on how to tell the difference between

the scam texts and the genuine ones from GP practices that are beginning to offer the vaccine.
Read the full article here

Self-Assessment tax returns: scammers posing as HMRC
With the deadline for self-assessment tax filing approaching on 31 January 2021, Which? have published an article detailing what you need to be wary of. With many small businesses and the self-employed heavily impacted during the pandemic, HMRC have issued a warning about fraudsters posing as the department. 846,000 suspicious communications have been referred to them in the past 12 months, 500,000 of these were relating to members of the public being offered bogus tax refunds.
Read the full article from Which? here

Pharmacist stuck off for defrauding the NHS of £76,475 by modifying scripts
A pharmacist in Wales has been struck off the General Pharmaceutical Council's (GPhC) register for committing fraud against the NHS, by claiming £76,475 from modifying over 1,500 prescriptions. The fraud, taking place at Talbot Pharmacy in Talbot Green, Wales, included claiming reimbursement for liquid medicines or dispersible tablets when in fact a cheaper alternative such as a tablet or capsule had been dispensed. The pharmacist was sentenced to 16 months in prison.
Read the full article here

CTSI warns of fraudulent phone calls targeting NHS employees
The Chartered Trading Standards Institute (CTSI) is warning NHS staff about a telephone-based scam seeking to gain their bank details. Towards the end of November, Scottish First Minister announced a one-off pro-rated payment of £500 for NHS staff and social care workers in Scotland. In December, health service workers in Scotland reported receiving calls from individuals claiming to be from the NHS asking for bank details to make the payment. The CTSI has warned that these calls are entirely fraudulent.
Read the full article here

Beware parcel delivery scams
The BBC has reported that criminals are looking to defraud customers by posing as well-known delivery companies. Fraudsters have been sending emails stating they have not been able to deliver goods and then asking for a fee to rearrange the delivery. They then try to extract financial details which are used to commit fraud.
Read the full BBC article here

Fraud risk warning: 'I was desperate for a job'
A recent BBC article reported the story of Helen Barker, who during a difficult time in her life was desperate for a job and fraudsters tried to take advantage. Ms Barker was looking for work within the care sector and she answered a job advert on a big recruitment website. She sent off an application form and other details, only to be informed that she needed to pay for a DBS check, ensuring she had no criminal convictions, as

well as training. Ms Barker had already sent a copy of her passport but was now being hassled for her bank card details to pay. Ms Barker realised it was a scam and managed to avoid losing any money.
Read the full BBC article here

PSNI fraud scam: Officer impersonator called people to ask for bank details
The BBC has reported that a scammer impersonating a fraud liaison officer from the Police Service of Northern Ireland (PSNI) is asking for people's bank details, the police have warned. The PSNI have said that the public need to be extra vigilant after a number of reports, including a request for the victim to leave their bank card in a post box.
Read the full BBC article here

Over £2million lost to criminals impersonating well-known broadband providers
Action Fraud has received reports of criminal's cold calling victims and pretending to be from well-known broadband providers. These calls claim that the victim has a problem with their computer, router or internet. The suspect persuades the victim to download and connect via a Remote Access Tool (RAT), allowing the suspect to gain access to the victim's computer or mobile phone. Some reports also state that criminals have been using browser pop-up windows to initiate contact with victims.
Read the full article from Action Fraud here

Which? released a digital guide to help people identify scams
Around the festive season, and into the new year, there is an increase in online shopping which creates the opportunity to fraudsters to create more scams and dodgy products. Which? has released a digital guide to help you spot and avoid scams, you can access the guide by clicking here.

Why not make scam awareness one of your New Year's resolutions?
Buckinghamshire and Surrey Trading Standards are pleased to be hosting 2 scam awareness sessions in January:

Friends Against Scams training session – 12th January 2021, 10:30 – 12:00, via Microsoft Teams
The "Friends against Scams" course raises awareness of scams and what to look out for and is aimed at anyone who would like to learn more about scams and how to deal with the different ones operating. After the course you will be recognised as a "friend" of the scheme and will be encouraged to talk to your friends and family about it, to help others become more scam aware.

AND/OR

ScamChampion training session – 13th January 2021, 10:30 – 12:30, via Microsoft Teams
Completed the Friends Against Scams session and wish to spread scam awareness further? Why not sign up to our ScamChampion course, where you'll be given the tools and resources to enable you to deliver the Friends Against Scams training to family and friends, colleagues,

communities or even as a volunteer for Trading Standards. You will need to have carried out the online FAS training prior to attending (http://www.friendsagainstscams.org.uk/elearning/surreybucks) or attended one of our live Friends Against Scams sessions, such as the 12th January course.

Please email natalie1.webb@surreycc.gov.uk to confirm attendance on each/either course, or if you'd like to find out about alternative dates!