COVID-19 Fraud & Security Alerts

Ref: CFMG-007

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

Local Fraud Alert - Fraudulent Invoice - Medical Supplies (COVID-19)

The Fraud and Security Management Service which is hosted by Hampshire and Isle of Wight Partnership of Clinical Commissioning Groups has issued a local fraud alert to: Hampshire and Isle of Wight General Practice Managers; Hampshire and Isle of Wight Chief Pharmacists; and NHS Trust/CCG Directors of Finance and Chief Finance Officers on 12 June 2020 regarding 'fraudulent invoices for medical supplies (COVID-19)'.

A general practice in the Hampshire and Isle of Wight area has reported that an invoice has been received from a company named as Med Supply Group LTD.

This company purports to be a supplier of medical supplies and had invoiced the general practice. These items had not been ordered by the practice and therefore the invoice is considered to be fraudulent with the aim of taking advantage of NHS financial systems during the COVID-19 national emergency. The company is registered with Companies House as a wholesaler of office furniture but no company website or online contact details have been located; other than those contained within the invoice which are given as medsupplygroup@dr.com and telephone 03300431276. You are urged not to use these details.

It is highlighted that the company's registered address is linked to a report made by the Insolvency Service in 2016 that identified a network of over 50 phantom companies. These companies were ordered into liquidation by the High Court on grounds of public interest and were reported as run solely as vehicles for fraud to obtain credit by filing false accounts and other false information.

Whilst it is not known at this stage whether Med Supply Group LTD is part of a wider concern, all NHS organisations should be vigilant when receiving any invoices or other contact from this company.

Action Required

1. General Practices should at the earliest opportunity undertake a review of their finance systems to ascertain whether any invoices have been received, paid or declined.
2. All NHS Trusts and Clinical Commissioning Groups should also conduct checks against their financial, procurement and ICT systems.

3. Any positive findings should be reported immediately to the LCFS.
4. All NHS organisations are advised to remain vigilant and be cautious if contacted by new suppliers. Any unusual requests should be reported or checked with line managers.

Shielding Patient Lists (SPL) – Letters

The NHS Counter Fraud Authority (CFA) has issued a document which sets out the process by which a person is flagged as clinically high-risk as well as identifying the vulnerabilities of shielding letters. The NHSCFA and Local Counter Fraud Specialists (LCFS) have received reports concerning the alleged use of fraudulent shielding letters for personal gain. These reports fall into the following categories:

- Staff alleged to be working when reporting to the self-isolating/shielding from their primary NHS role.
- Staff member reporting they are self-isolating/shielding following the receipt of a shielding text. Text is believed to be fake and staff member reports they have not received a letter and reports GP has refused to provide a shielding note.
- Staff member has provided what is believed to be a fake letter shielding letter. Checks with staff member's GP confirms the letter is not authentic.
- Staff member believed to be self-isolating/shielding but seen outside of their home socialising.

The full document is available on the NHSCFA Extranet which is currently available to Local Counter Fraud Specialists and Directors of Finance.

Avoid identify theft

NHS Digital has provided some advice on how to avoid unauthorised access and theft of your identify. When sharing your identity online you are risking theft of your identify. Here are NHS Digital's top tips:

- Don't upload images of your work pass online.
- Uploading a selfie? Then take off your pass.
- Remove your NHS ID when you're not in the workplace.
- Remove your pass for work photos.

NHSmail phishing incident

NHS Digital is working closely with the National Cyber Security Centre, who are investigating a widespread phishing campaign against a broad range of organisations across the UK. This has affected a very small proportion of NHS email accounts. Further information can be found here. The NCSC has confirmed that this activity is part of a widespread credential-harvesting phishing campaign that is targeting a broad range of organisations across the UK.

NHS Test and Trace

NHS Test and Trace emails continue to be a target for fraudsters. Criminals are now using the NHS Test and Trace service as an opportunity to gain access to your home. The Chartered Trading Standards Institute (CTSI) has witnessed evidence of bogus texts informing members of the

public that a "COVID Home Testing Team" will visit their homes. NHS Test and Trace will never ask to visit your home. Read full article here
There are many news articles regarding fake emails and guidance on what to look out for. The fake email refers to the service as 'track and trace' and advises the recipient that they have been exposed to someone who has tested positive for coronavirus. They are instructed to click a link to find out who that person is and warned if they fail to do so within 24 hours, legal action may be taken and benefits suspended. The email address used is alert@nhs-trackandtrace233-gov.com.
Fraudsters may also try to exploit the government's new test and trace system by spoofing the telephone number used by contact tracers and use this to talk individuals into providing personal/financial details.
There is a useful guide here to the system, issued by the government, on how it works and what to expect if you are contacted. The key advice is that NHS contact tracers will **NEVER** ask you to:

- dial a premium rate number to speak to them (e.g. those starting 09 or 087).
- make any form of payment.
- purchase a product or any kind.
- details about bank accounts.
- give social media identities or login details, or those of contacts.
- supply any passwords or PINs, or set up any passwords or PINs over the phone.
- disclose any of your personal or medical information to your contacts.
- download any software to your PC.
- hand over control of your PC, smartphone or tablet to anyone.
- access any website that does not belong to the government or NHS.

Cybercriminals are targeting Hospitals during COVID-19 – simple steps can protect you

Bad actors are identifying healthcare systems as a particularly desirable target with hospitals in Spain, France, the Czech Republic and Israel all having suffered known cyber-attacks since the start of the pandemic. Interpol recently released a global alert to healthcare organisations warning that criminals are attempting to use ransomware attacks to lock users out of their own systems. The healthcare sector has always been vulnerable to cyber-attacks. This was seen most prominently in May 2017 when the WannaCry ransomware attack paralysed parts of the NHS. Although personal devices are coming onto the network sporadically and create security headaches, new medical devices are also vulnerable to attacks. With so many companies banding together to help defeat the virus by donating or quickly building ventilators, there will be hundreds, even thousands of new devices connecting to hospital networks. The BBC TV show Holby City, for example, had real ventilators on set and has now donated them to the NHS. Although these machines will save lives, they could potentially be the cause for a major cyber-attack and a way in for bad actors trying to cripple the health system. IT teams struggle to keep up with all the new devices being connected to hospital networks, they need to ensure that they have a solution in place which allows them to have a holistic view of all devices, the operating systems

they are running on and whether they have installed the latest updates or not.
Read the full article here

DHL Scam email

An Accounts Manager at a Trust has received three emails in quick succession appearing to be from DHL. The Trust does have had an account set up with DHL but it has never been used and the emails were sent to a named person in the Accounts Team who has never had dealing with DHL. The emails have been in the format below:

DHL Accounts Dept. <noreply@dhl.com>
Mon 08/06/2020 16:34

Dear Customer, Please find attached letter concerning your overdue account This is a system generated email. Please do not respond to this email. Invoice Copies can be retrieved from MyBill If you have any questions or concerns, please email billing.help@dhl.com. Regards, DHL Express Accounts Dept.

If you receive a similar email from DHL, please do not click on attachments and contact DHL directly via a known phone number or email address to confirm whether there are any outstanding invoices.

DHL have been contacted about this issue.

Romance Frauds

Last week the alert reminded people to be aware of fraudsters posing as nurses on dating sites. The East Midlands Special Operations Unit (EMSOU) has produced additional information on 'Romance Frauds' as follows:

Romance fraud is in the top five most commonly reported scams to Action Fraud and cost the UK £27 million last year, according to the latest stats from the National Fraud Intelligence Bureau (NFIB) and Get Safe Online .

Romance Fraud involves feigning romantic intentions towards a victim, gaining their affection and trust, and then using that goodwill to access the victim's money, bank accounts, credit cards or forcing the victims to commit financial fraud on their behalf. They may also collect personal details for identity fraud.

Example:

In February and March of this year, Ms Brenda Parke, a 60 year old retiree, was scammed out of £60,000 after joining an online dating site and befriending a man calling himself Bradford Cole.

Bradford portrayed himself to be a successful Dutch businessman and whilst abroad on business, his daughter was injured in a hit and run accident and required £9,600 for an operation. Bradford subtly and cleverly manipulated Brenda into taking a position of responsibility for his daughter's welfare. Later on, he managed to secure a further £44,500 for his ailing business and then further monies for his accommodation

and transport home.
Ms Parke, an otherwise cautious and sensible individual, was expertly manipulated and her full story can be found here.
This type of fraud is a multi-billion pound worldwide business conducted by lone individuals and large scale criminal organisations.

Warning signs

Fraudsters adopt a variety of tactics and may:

- Ask to move communications away from dating websites to instant messaging, text, email or phone calls.
- Ask a lot personal questions but reveal little about themselves, or their details don't quite add up. Say they're university educated, but spelling and grammar are poor.
- Try to establish a bond quickly, by using an endearing pet name or claiming that 'they've never felt like this before'.
- Promise to see you, but cancel every time or offer excuses which delay meeting up, like financial troubles.
- Request money for emotive reasons such family illness or hardship.

How to protect yourself

- Don't trust people too quickly – be cautious and trust your instincts.
- Protect your privacy, do not reveal too much online, especially on social networks.
- Never send money to people you have not met.
- If you use internet dating, keep all communication via that website.
- Perform a reverse image search of their profile photo, does it belong to someone else?

Further advice from Action Fraud can be found here.
(EMSOU)

Spyware

The East Midlands Special Operations Unit (EMSOU) has provided the following information regarding 'Spyware':
'Spyware', refers to a category of software that, when installed on a computer, may send pop-up ads, redirect your browser, or monitor the web sites visited. More invasive versions of spyware can even record what is typed on the keyboard. Spyware may cause a computer to become slow or sluggish. There are also privacy implications including:

- What information is being gathered?
- Who is receiving it?
- How is it being used?

Spyware that record keystrokes, passes, important credentials and sensitive data to malicious threat actors to exploit for personal gain (identity theft, fraud etc.).
Symptoms that indicate spyware is installed on a computer may include the appearance of new and unexpected:

- Toolbars in the web browser
- Icons on the toolbar at the bottom of the screen
- Search engines employed by the browser
- Home page
- Pop-up windows
- Random Window error messages

Other indicators may be:

- The computer suddenly becoming sluggish (for example, when saving files).
- Being redirected to web sites other than the one entered into a browser.

Mitigation strategies

Be wary of:

- Links within pop-up windows: These windows often install spyware. To close a pop-up window, click on the "X" icon in the title bar and not the "Close" button within the window.
- Unexpected dialog boxes: Which asks to run a program or perform another type of task. If in doubt, select "no" or "cancel," or close the dialog box by clicking the "X" icon.
- Free software: There are many sites offering customised toolbars or software that will appeal to users. Downloading programs from untrusted sites may expose you to spyware.
- Following email links for anti-spyware software: Like email viruses, these links may serve the opposite purpose and actually install the spyware it claims to be eliminating.

Also consider adjusting browser preferences; to limit pop-up windows which contain active content, which can be harmful. Certain types of cookies can reveal what pages a user has visited. Rather than deny by default, most browsers allow the user to fine tune which sites can use cookies so that the overall surfing experience is not adversely affected.

Removing spyware

Run anti-virus software for detection and removal. If problems persist run legitimate spyware removal tools from, trusted vendors. Be careful that the spyware removal software is compatible with the existing anti-virus software. Always keep anti-virus software up to date and update your systems.

Citizens Advice scam awareness

Citizens Advice have reported that over a third of British adults have been a victim of a scam during Lockdown and the charity reported a 19% increase in the number of people coming to their website for scam advice. Of those with a disability or long term illness, 45% said they had been targeted, while half deemed at an increased risk of coronavirus or shielding had been contacted. Some 54% who have been affected by loss of

income during the pandemic said they too had been confronted with a con. If you see emails or texts about coronavirus from someone you don't know, or from an unusual email address, don't click on any links or buy anything. Read article here
Click here for the Citizens Advice online scams helper

2,378 victims have lost a combined total of over £7m to coronavirus-related scams

Action Fraud have reported that as at 12 June 2020, a total of £7,099,441 has been reported lost by 2,378 victims of coronavirus-related scams. Action Fraud have received 12,323 reports of coronavirus-related phishing emails. Criminals continue to exploit the coronavirus pandemic to defraud innocent members of the public. Currently, coronavirus-related frauds make up less than 2% of all fraud reports received. To keep this number as low as possible, Action Fraud wants people to be aware of the very simple steps they can take to protect themselves from handing over their money, or personal details, to criminals.

Over £16 million lost to online shopping fraud during lockdown, with people aged 18-26 most at risk

Action Fraud is warning the public to remain vigilant and take extra care when shopping online. Since shops were forced to close due to the coronavirus outbreak on 23 March, Action Fraud has received reports of online shopping fraud totalling £16.6million in losses.

To protect yourself from falling victim to online shopping or auction fraud remember the following:

- Where to shop – carry out research if new company or seller.
- Email accounts - use strong, separate password for your email account.
- Phishing - be cautious of emails or texts about amazing offers containing links to fake websites. Try and avoid using links and type the website directly into your browser instead.
- Payment method – Use a credit card if possible.
- Do your research – Find additional information on how to shop online safely here.

Read full article here

Australian Cyber Attack targets government departments including healthcare

The BBC has reported today that a range of Australian government departments and institutions are experiencing an on-going cyber-attack. The article reports that Australian Prime Minister Scott Morrison has stated the sophisticated attacks had been identified as state backed, but did not identify which country was suspected. The attacks include health care organisations along with educational and political organisations. The Prime Minister has urged organisations and businesses, especially those involved in health infrastructure and health service providers to improve technical defences.
Read the BBC article here

Furlough fraud confessions

The Telegraph have reported this week that HM Revenue and Customs are planning to crease a 30 day window for companies to confess

breaches of the governments furlough scheme. The article reports that since March, £19.6bn has been paid out to almost nine million furloughed workers. With an additional £7.5bn paid out to self-employed workers. In previous alerts we have highlighted the increased press coverage around furlough fraud as employees report companies for breaching rules. It is thought that following the 30 day window, HMRC will actively pursue companies by criminal and civil powers.
Read more here
In a separate article, The Telegraph highlights a recent report found one in three workers on the furlough scheme have been fraudulently asked to work.
Read more here

Advertising watchdogs join forces to target online scams
A partnership between the Advertising Standards Authority and Internet Advertising Bureau has created a new site allowing the public to report scam advertisements online. The Telegraph report that the joint partnership would allow details of a scam advertisement to be shared amongst all affected platforms. During the initial trial period, scam adverts were removed on average within two days.
Read more here

Avoid scoring a cyber own goal when streaming Premier League's return
The National Cyber Security Centre (NCSC) is urging football fans to secure their online platform streaming accounts and subscriptions. FOOTBALL fans have been warned of cyber threats when they swap their tickets for TV subscriptions – and been advised how to watch behind-closed-doors games as safely as possible. The NCSC has shone a light on online criminals who could hack into accounts by guessing passwords that are obvious or have been compromised in the past. Last year the NCSC exposed the most compromised passwords in the world; almost 700,000 accounts have been compromised through hackers guessing a device's passwords as 'liverpool', 'chelsea' or 'arsenal' and 23.2 million accounts breached by hackers guessing the password '123456'. Fans can secure their viewing experience by: refreshing accounts; setting a strong password; and updating streaming apps.
Read full details here

Webinars:

- The Cyber Academy Webinars: COVID-19 fraud online on Thursday 25 June 2020 at 13:00 – 14:00.
  This free webinar is open to everybody. The webinar will examine some of the most effective ways criminals are disguising their activities, how quick they are to respond and how easily they adapt when they are discovered and their websites are blacklisted by search engines and cyber security tools.
  Read here for more details and to register

Other type of fraud examples

Ransomware

- Claire's Accessories online site checkout page was hacked by insertion of a malicious "card skimming" code which collected payment card information. The retail giant admitted that the malware gained access to payment card information from its e-commerce website but assured customers that cards used in retail stores were not affected by the issue. Any customers, who made purchases on Claire's website between 30 April and 13 June 2020, should contact their card company and monitor statements for fraudulent purchases.
- Cycling equipment shop Wiggle were also targeted in this type of attack and a small number of customer details were acquired. In response, Wiggle have taken steps to identify the compromised accounts and contact the individuals impacted. All accounts will now require the re-entry of card details for the next purchase. Wiggle customers are strongly advised, to change login passwords and check any cards previously used to make purchases.

Email scams & Phishing scams

- Black Lives Matter Phishing Email: Members of the public have been targeted by a phishing attack going out with the subject line: 'Vote anonymous about 'Black Lives Matter'. There is little to no content in the email except the statement: "Leave a review confidentially about Black Lives Matter... Claim in attached file." When the recipient clicks on the attached file it installs a dangerous Microsoft Windows malware known as 'TrickBot'. During the protests and pandemic criminals have continuously exploited these current events to target members of the public. Members of the public should always employ caution when receiving unsolicited emails and never click or open attached files or links in those emails. (Cifas)
- Cifas has warned that hackers target Bluetooth users: The use of Bluetooth is increasing as means of transferring files between laptops and phones with so many working in remote environments. Hackers have found multiple ways of hacking using Bluetooth to gather important data (texts, photos, cell provider, ISP, etc), attack users with spam advertisements, and even bug devices. The best ways to avoid falling victim is to avoid using Bluetooth to communicate sensitive information like passwords and document. If you must use Bluetooth you should encrypt your files first. Only leave your Bluetooth in "discoverable" mode when you're pairing a new peripheral with your phone or laptop, there is no need if using the same device ie headphones. And overall, you should turn Bluetooth off when you're not using it.
- Phishing emails have targeted customers of the media streaming service Netflix in recent weeks. Similar to previously reported TV License emails, the communications report payment details have failed. The email contains a link for the recipient to update payment details. Guidance on how to identify genuine communications are available on the Netflix website.
- New HMRC text message phishing scam targets self-employed. A new phishing scam, designed to steal personal and financial details from self-employed workers using the Self-Employment Income Support Scheme (SEISS), has been uncovered by litigation company Griffin Law. Victims are informed via SMS that they may be eligible for a tax refund and are redirected to a website that looks like the official HMRC site. From there, victims are asked to provide personal data including email address and HMRC login details. A fake refund

amount then appears before victims are redirected to another page that asks for financial information such as account number, security code and expiry date, to claim the bogus amount. HMRC will never send notifications of a tax rebate or ask that personal or payment information be disclosed by email or text message. Read full article here
The NCSC has also issued further information on how self-employed workers, and others, can protect themselves against these scams of this type. Read here

Phone and Text Scams

- Cifas reports of calls coming from your "bank" saying there has been suspicious activity on their accounts. The number from the call has spoofed the number on the back of the card. Remember to #takefive and don't be afraid to contact your bank via the number on the back of your card.

Social media and other messaging platforms

- Android users have been warned that the app SnapTube may be taking money from their accounts without them knowing. The app allows users to download videos from sites like YouTube and Facebook. It appears that once downloaded, the app can sign users up for premium services without them knowing - and this can prove to be very costly. These scams work by the apps downloaded from the Google Play Store can take payments from linked bank cards. Whilst not technically malware, this type of scam app has been labelled 'fleeceware', since it can fleece unwitting people out of cash. Read article here
- Southwest Airlines Facebook scam: Facebook users found alleged advertisements from Southwest Airlines, offering 100% free round-trip flights for the first 500 people who shared and commented on the posts. This is a common scam often seen on social media sites. Many fall for the scam believing it is a giveaway and fun way for businesses to keep loyalty amongst customers. But the main purpose for many of these pages, posts, giveaways and quizzes, is to harvest personal and financial details from as many people as possible.

Spoof websites / emails

- Job Advert Scam: During these uncertain times many individuals are looking for new or additional jobs and fraudsters are attempting to exploit these people. A job advert scam is being conducted by fraudsters using a legitimate job advert website. Victims applying for the role are asked to attend an interview over video conference and at the end of the interview are told they will receive a Business Credit Card. The card duly arrived with the applicants name on it and they are instructed to purchase online vouchers and send the voucher codes back to 'employer'. Unbeknown to the victims the fraudsters have set up the card using the victim's personal details and mobile number but the fraudsters email address. (Cifas)
- Universal Credit scams: Many people are being targeted by scammers offering government loans and grants linked to Universal Credit

claims. Some of these scammers come prepared with professional looking social media profiles and websites, with testimonials and government logos. DWP will never text or email asking for your personal information or bank details. Anyone who thinks they have been a victim of fraud should report it to Action Fraud, and notify DWP, as soon as possible.