COVID-19 Fraud & Security Alerts

Ref: CFMG-001

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

Fraud in Emergency Management

In times of emergency it is important that resources and funds get where they are needed as quickly as possible. In response to the current COVID-19 pandemic, policies and processes may have been relaxed to get resource to where it is needed. The provision of emergency relief and services has an inherently high risk of fraud, and is a prime target for those seeking to make a gain at the expense of others. It is important that those leading the creation and administration of this support are made aware of the threat posed by fraud and are able to make conscious decisions on which risks are to be tolerated. To aid these decisions the International Public Sector Fraud Forum has issued a paper entitled *Fraud in Emergency Management and Recovery*. The paper describes what is meant by emergency management, why emergency management has an inherently high risk of fraud and why we should care about it. You can access the paper here, however, the paper highlights the following control principles:

- Accept that there is an inherently high risk of fraud, and it is very likely to happen.
- Integrate fraud control resources (personnel) into the policy and process design to build awareness of fraud risks.
- The organisation and fraud control should work together to implement low friction counter measures to prevent fraud risk where possible.
- Carry out targeted post-event assurance to look for fraud, ensuring access to fraud investigation resource.
- Be mindful of the shift from emergency payments into longer term services and revisit the control framework – especially where large sums are invested.

(Reference: International Public Sector Fraud Forum, 2020)

COVID-19 Fraud and Security Risks (Cyber - Online Scams)

The rise in online communication can heighten vulnerability to cyber, data security and privacy threats. Cyber criminals will actively look to exploit these threats. In fact, COVID-19 related fraud reports increased by 400% in March 2020. The National Fraud Intelligence Bureau reported a new trend in fraud related to COVID-19. Updated figures show that there have been 105 reports to Action Fraud since 1 February

2020, with total losses reaching nearly £970,000. The majority of reports are related to online shopping scams where people have ordered protective face masks, hand sanitiser and other products which have never arrived. It is likely that these scams will extend into the NHS working environment.

In order to mitigate this risk the organisation should ensure that all staff are logged on through a VPN when working remotely and all staff should use NHSMail accounts, particularly when transferring sensitive data between insecure environments. The NHS Fraud and Security Management Service have issued this guidance which sets out the principles that should be followed:

- always lock your computer when you are away from your keyboard, even for a short time.
- never share your password with anyone.
- do not plug non-NHS hardware (e.g. phones, memory sticks etc.) into your computer.
- do not leave laptops or NHS phones in your car, if it is unavoidable then lock them in the boot.
- do not use public Wi-Fi – as soon as you connect your password could be collected by a criminal using dark web software.
- keep your computer and phone software upgrades up to date.

All spam emails received through NHSMail should be reported to spamreports@nhs.net.

(Reference: NHS Fraud and Security Management Service, 2020)

NHS Counter Fraud Authority (NHS CFA) Guidance

The NHS CFA recently launched an expanded NHS Fraud Reference Guide. The guide is a simple but essential way in which you can help in knowing how to spot NHS Fraud. It contains information on different types of NHS fraud and preventative advice, case studies and further resources. The guide contains new sections such as a detailed look at 13 key areas of fraud, information on how to spot fraud, case examples and preventative advice. Click here to read the guidance in full

In addition the CFA have also produced Covid-19 counter fraud guidance. This guidance and advice is available to help mitigate the risk of fraud and protect NHS resources during the COVID-19 pandemic and covers mandate, procurement, recruitment, payroll, and personal fraud risks. Mandate fraud provides advice and guidance for the NHS on how to mitigate the risk of mandate fraud and CEO/payroll email fraud during the COVID-19 pandemic. The procurement fraud guidance covers onboarding new suppliers, procuring goods, services and works with existing suppliers, managing contracts and performance and paying suppliers. The recruitment fraud information covers updated recruitment guidance during the pandemic, verification of documents, identity checks, right to work, criminal record checks and references. The payroll guidance specifically focuses on timesheets, expenses, sickness and absence. Advisory guidance is provided for all NHS staff and includes awareness of the personal fraud risks during the COVID-19 pandemic. All guidance pages provide an overview of the fraud risks within the topic along with what should be done to reduce the risk. Click here to read the guidance in full

Covid-19 Cyber and Fraud Protect Messages (Zoom conference calling)

Zoom is a video chat platform, which has received quite a lot of adverse publicity because of a number of important security flaws. Criticism included uninvited people joining your conversation to deliver racist messages or pornographic images, to poor encryption methods that mean private conversations are not always private. The guidance below from East Midlands Special Operations Unit (EMSOU), part of the East Midlands police forces, has been written for home and business, to help keep secure:

What to Do

- Make sure you have the latest version of the Zoom software. Click your user icon and select 'Check for Updates'. Usually, updates fix known security flaws.
- Running anti-virus software or a firewall on your computer and keeping software up-to-date will improve your security.
- If you are holding public meetings, where anyone can join the conversation, be sure to configure screen-sharing settings.
- Go to 'In Meeting (Basic)' and select 'host alone can share' or turn off screen sharing entirely. This can also be controlled by the host during a meeting.
- Finally, turn of 'Annotation', if you are worried about how people might annotate your shared slide show.

Stop Uninvited Guests

- Setting up a Zoom meeting creates a **9 digit ID**. Anyone who has this ID can join the conversation. **Don't advertise it publicly by posting it on Social media.**
- If you use the '**Options Panel**' when setting up a meeting, you can add an **access password** too. Would-be trolls now need an ID and a password to gate crash your meeting.
- Use the '**Advanced Options**' to enable a '**Waiting Room**'. This puts people in a holding area before you grant or deny them access to your conversation.
- Organisers can lock the meeting once everyone who needs to has joined. Click **Manage Participants** >> **More** >> **Lock Meeting**.

Stay Private

- The organiser of a meeting can record audio and video from the meeting. Also, anyone involved in a '**private chat**' can save this as a log file.
- Turn off video and mute yourself unless needed. This prevents video recording conversations in your home or exposing information inadvertently.
- It is possible to encrypt your video calls in the settings panel, which will improve the confidentiality of your conversations. Be aware,

however that there is no certainty as to whether this is end-to-end encryption.

- Accessing Zoom through the browser is more secure than downloading the app. The feature is available on the log in screen when invited to a meeting, although hard to spot.

Always Be Aware

- Your conversations may not be as private as you would like. Is Siri, Alexa or Google assistant in range? They will ALWAYS be listening and passing info back to their servers to maintain the connection and sampling purposes.

Final Thoughts

- Whatever platform is chosen it is vital that all the security settings are reviewed and implemented as appropriate.

In circumstances where sensitive or confidential discussions are being held other providers, such as Google Duo, Skype, Face Time, WhatsApp and Webex might be alternatives.

(Reference: EMSOU Covid-19 Cyber and Fraud Protect Messages)

Vishing

Vishing is actually a combination of two key terms 'voice' and 'phishing'.

Phishing uses deception to get an individual to reveal personal, sensitive, or confidential information, such as bank details or account passwords. Instead of using regular emails, or fake websites like phishers do, vishers use an internet based telephone.

Keep vigilant:

- **Keep abreast of the news:** Knowledge of attack methods and techniques will hone the ability to separate fact from fiction.
- **Understand:** A legitimate business won't make unsolicited requests for personal, sensitive, or financial information. Anyone who does this over the phone is probably trying to scam you.
- **Call back using official channels:** No matter how friendly or stressful the call might seem, ask yourself, 'how can I contact the company or an official representative through official, well known, channels?' Once you know the correct communication channels, verify the claims being made.
- **Don't give into pressure:** If someone tries to coerce you into giving them sensitive information, hang up.
- **Use Telephone Preference Service (TPS):** Register your number with the TPS to prevent unwanted sales and marketing calls.

(Reference: EMSOU Covid-19 Cyber and Fraud Protect Messages)

NHS Tracking App

The NHS tracking app has generated debate over privacy and security concerns, however:

- The app does not collect your personal data so you remain anonymous.
- The app does not collect personal details of anyone you interact with.
- App data is encrypted.
- When anonymous data is uploaded to the NHS, the systems used are said to be secure. Not enough information is collected to specifically identify individuals.

Click here for further information

(Reference: EMSOU Covid-19 Cyber and Fraud Protect Messages)

Procurement Fraud

NHS England/Improvement recently issued guidance to health bodies allowing prepayment of goods and services during the pandemic. Prepayment can only be exercised in extremely limited and exceptional circumstances. The guidance can be found at this link: Click here to read the NHSE/I guidance

Guidance has been issued by CIPFA to remind organisations to protect the supply chain from fraud. The information is a reminder of the continuing risks to supply chains posed by fraud and corruption, many of which are exacerbated by emergency circumstances. This guidance can be found at this link: Click here to read the CIPFA guidance

Password Security

- Passwords are used widely and include accessing personal computers and computing devices and services of all kinds. While protecting them from attackers who might read, steal or even destroy sensitive data. For password tips and system user tips and more detailed guidance on passwords, from the National Cyber Security Centre (NCSC), can be found here.

National Cyber Security Centre Issue warning to Healthcare Organisations

On 5 May 2020 the NCSC issued a warning to key healthcare organisations, following the UK and US revealing campaigns against healthcare organisations including policy makers and researchers. Both the NCSC and US Cybersecurity and Infrastructure Security Agency (CISA) have reported 'password spraying' campaigns against healthcare bodies and medical research organisations. Following the guidance noted above on password security, the NCSC has advised staff to change passwords that can by easily guessed with three random words and implement two-factor authentication. Click here to read the NCSC alert

NHS Nightingale Construction Companies Targeted by Cyber-attack

It has been reported by Info Security Magazine that two national construction companies involved in building the NHS Nightingale emergency

COVID-19 hospitals have been targeted by cyber-attacks. It is reported that Bam Construct UK, which built the NHS Nightingale hospital in Harrogate, Yorkshire was targeted by a ransomware attack. Whilst Interserve, which supported on the construction of NHS Nightingale Birmingham suffered a data breach.
Interserve have released a press release stating that they are working with the NCSC and has informed the Information Commissioner's Office (ICO). In addition, the statement notes "Interserve's employees, former employees, clients and suppliers are requested to exercise heightened vigilance during this time." Read the full article here

NHS Charities Together Text Scam

Employees within the 360 Assurance client base have reported receiving a phishing text that reads: 'Donate to the NHS Charities Together Covid19 Fund and receive a home testing kit free of charge.' The sender is 'NHSFund'. If you receive this text message please do not click on the link as the text message is fraudulent.

Man Who Claimed To Have Had Covid-19 Jailed After Coughing on Derbyshire Police Officers

The incident happened on Thursday, 2 April, when Derbyshire Police were called to a canal path in South Derbyshire, following reports from members of the public that a man was being abusive and threatening. When the officers arrived, they found a man carrying a 2' piece of wood and waving it above his head in a threatening manner.

He was arrested and the piece of wood taken off him. Whilst the officers spoke to the man and asked if he was, or had been suffering from the virus, he replied: "I've already had it, I've got over it and now I am a super spreader so…" He then coughed in the direction of the three officers.

Christopher McKendrick, who is 58-years-of-age and lives in Swarkestone, was arrested. He was later charged with the offences: common assault, possession of an offensive weapon in a public place, assault by beating of an emergency worker and using threatening, abusive, insulting words or behaviour to cause harassment, alarm or distress.

Mr McKendrick appeared at Southern Derbyshire Magistrates' Court on Friday 3 April where he pleaded guilty to the offences. He was jailed for a total of 16 weeks and ordered to pay a victim surcharge of £122.

Read the full article here

Nurse committing internal fraud

A nurse in USA caring for an elderly Covid-19 patient has been accused of using the patient's credit card for a number of purchases. This is a reminder that internal fraud is always a threat even in crisis - unfortunately some will take advantage of any situation for financial gain. Employers should look to support employees who have been impacted in any way during these times and could end up in financial difficulty –

some may see no way out other than to steal or commit fraud.
Read the full article here

Other type of fraud examples

Ransomware

- Report received of a cyber-attack on a business in which the computers had remote access enabled, which made the network more vulnerable. The attack shut off each computers anti-virus software, then infected the computer with ransomware.

Email Scams – Phishing emails

- The Fraud Advisory Panel reported that 18.5% of emails to the phishing inbox were COVID related.
- UK Government free school meal scam emails, stating the following: 'As schools will be closing, if you're entitled to free school meals, please send your bank details and we'll make sure you're supported'. The UK Government has confirmed this is a scam email.
- UK Government COVID-19 funding scam email, requesting funding donations to the NHS. A similar email reportedly from the World Health Organization also asking for funding.
- Emails and calls claiming to be from a payroll department requiring recipients to verify personal details. The link provided provides an opportunity to steal email logins, passwords and personal details.
- Bank phishing emails purporting to be from HSBC Bank. The communication claims to be providing all customers with £500 due to the pandemic. Other banking emails state the recipients account is compromised and require a new account to be created or funds to be transferred.
- UK Government COVID-19 relief form, email requests completion of the form in order to receive payment within 2 days
- PayPal phishing email campaign has recently been identified, which is convincing and is personalised to the recipient. The communication includes corporate messaging on Coronavirus.
- Scam emails purporting to be from beer producer Heineken promoting a giveaway of free kegs of beer.
- A new Phishing campaign has been found that not only impersonates a company's management team but also suggests that a fellow employee has tested positive for COVID-19. The email then urges recipients to read an enclosed malicious attachment titled as "guidelines" or "next steps" to follow and when opened installs malicious software.
- TV Licensing scam emails, in which the recipient is advised they are eligible for six months of free TV Licensing, due to COVID-19, also claim the recipient's payment has failed and they need to renew now in order to avoid prosecution.
- Emails using Her Majesty's Revenue and Customs (HMRC) branding asking recipients to send copies of their passport, utility bills and bank

statements via a link to an infected site. Other variants of HMRC branded emails target businesses in relation to tax returns and the Coronavirus Job Retention Scheme, both emails divert to fake websites to obtain personal details.

- Amazon Prime emails report to changing pricing from £7.99 a month to £79 each quarter. This has been confirmed as a scam by Amazon.
- Reports received of emails purporting to be from Virgin Media, informing recipients that their bill is ready. The emails include information on how Virgin Media are responding to the COVID-19 outbreak. The bill amount commonly equates to £60.78.
- Also emails purporting to be from the Virgin Media e-billing team, advising recipient that their account will be frozen because their bank details couldn't be validated. Recipients are asked to click on a link to re-validate and amend their billing details. The link provides an opportunity for fraudsters to steal email passwords and personal details.
- Fraudsters send victims own passwords in sextortion scam. The National Fraud Intelligence Bureau reported a total of 9,473 phishing emails linked to sextortion have been made between 31March 2020 and 19 April 2020.
- Spoofing messages from the UK's largest mobile phone network to try and steal personal information. The emails use the official EE mobile network provider imagery, luring victims with the subject line "View Bill –Error", and report that there has been an issue with the customer's payment urging them to update their details with EE. Once victims click the fraudulent link they are taken to a phishing page.
- Customers of Drive DeVilbiss Healthcare (a leading manufacturer and distributor of medical products) have been receiving scam emails stating that that they have changed their bank details and instructing them to pay all outstanding invoices into a new bank account.
- An email, claiming to be from the Department for Work and Pensions (DWP), tries to gain debit or credit card details from the individual by saying that they are entitled to a council tax refund. Individuals are encouraged to click a link and leave their card details for the refund to be made. If you receive such message contact your council to confirm via a secure and confirmed phone line or email address, do not reply to the suspicious email or click any links.
- Scam delivery message from parcel service DHL stating, "Hey, here's how to track your delivery," are being received y individuals. This is the sort of message you might reasonably expect when you order something, however clicking the link brings recipients to a fake DHL website. These websites are then used to harvest personal information or banking details which can then be used to commit further fraud. Delivery messages should be treated as notifications only and links ignored – make a note of the right website to use for tracking the item, then search through your browser.

Online Retailers / Counterfeit goods

- Rogue traders trying to sell items such as face masks, sanitisers, thermometers, immunity oils and testing kits.
- An investigation supported by Europol focuses on the transfer of €6.6 million by one company to another company in Singapore in order to purchase alcohol gels and FFP3/2 masks. The goods were never received.
- In one 24 hour period losses of £72,154 have been reported from people who have purchased large quantities of face masks online which

have not been delivered.

- Victim is persuaded by the suspect to make an advanced payment for a rental property. The suspect uses the outbreak as the reason for the victim being unable to view the property. The property does not exist.
- Suspect advertises a pet online (puppy or kitten) and uses the outbreak as a reason the victim can't come and see the animal. The suspect sends photos and persuades the victim to make payment in advance. The suspect never provides the pet.
- Between 3-10 March 2020, over 34 000 counterfeit surgical masks were seized by law enforcement authorities worldwide.

Door to Door Fraud

- Rogue traders trying to sell items such as face masks.
- "Good Samaritans" offering to do shopping for the elderly and vulnerable which ends on them making off with a cash card and pin number.
- People impersonating officials gaining access to homes by saying they are offering COVID-19 testing.
- Increase in cases of fake charities knocking on doors and asking residents to donate to coronavirus related causes.

Spoof websites / emails

- A hoax copy of the NHS website has been discovered. The website includes harmful links to COVID-19-related health tips. Once these links are clicked on, a pop-up box appears asking visitors to save a file called 'COVID19'. If saved, the malware it contains steals passwords, credit card data, cookies from browsers, crypto wallets, files and screenshots.
- Pizza-Hut have identified that scammers are taking advantage of the COVID-19 lockdown to set up multiple fake sites using its brand name to lure the unsuspecting into giving bank/card details. The addresses of the fake sites — which strongly resemble the authentic Pizza Hut web-based ordering platform — include 'http://pizzahutaccount.com' and 'http://pizzahut-service.co.uk'.
- A spoofing campaign has been identified which uses socially engineered emails promising access to important information about cases of COVID-19 in the receiver's local area.
- Cyber-thieves are impersonating videoconferencing platform Zoom to steal victims Microsoft credentials. New research revealed that Zoom users are being targeted with fake notification emails that contain malicious links. When the user clicks on the legitimate-looking Zoom link they are taken to a fake Microsoft login page with the name of the user's organization and "Zoom" above the sign-in location. The attackers attempted to disguise their location by using many different Virtual Private Network (VPN) sources, the messages all look similar, were sent during a short, discrete time period, and use the same VPN services.

Text Scams

- A text scam is doing the rounds, which is attempting to fool people into believing they have been in contact with someone who has tested positive for the virus. The scam text reads: “Someone who came in contact with you tested positive or has shown symptoms for Covid-19" and then recommends that you self-isolate and/or get tested including a link. These texts are a way to steal personal data and may put the bank accounts of recipients at risk.

Password

- Healthcare bodies, medical research organisations, pharmaceutical companies, academia, and local governments have been targeted. Most of these attacks used password spraying (an attack that attempts to access a large number of accounts with a few commonly used passwords) to gain access to a large number of accounts. Europol reported that the Czech Republic highlighted a cyber-attack on Brno University Hospital which forced the hospital to shut down its entire IT network, postpone urgent surgical interventions and re-route new acute patients to a nearby hospital.