COVID-19 Fraud & Security Alerts

Ref: CFMG-0011

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

Health bodies show improvement in managing their fraud risks

The NHSCFA Quality and Compliance Unit undertook a two-phase thematic exercise, during the 2019-20 financial year, against standard 1.4 of their standards for fraud, bribery and corruption to measure the level of fraud risk assessment undertaken across 500 organisations in England and Wales.

The report from the exercise sets out the background, objectives, scope, methodology and findings of this work, which took place in two phases (early 2019 and early 2020). This report also sets out what the NHSCFA intends to do to support colleagues in fraud risk analysis moving forward to ensure that the methodologies and requirements of the Government Counter Fraud Functional Standard can be met.

The findings of the report indicate that following support from the NHSCFA during 2019 through a series of awareness workshops and the endeavours of our colleagues providing the counter fraud service, there has been a substantial improvement in fraud risk management within organisations. Following the risk awareness workshops there was a 130% increase in the number of organisations recording fraud risks in line with their own risk management policies (up from 138 organisations to 317). This is a positive outcome from the exercise and feedback from the LCFS community also suggests that LCFSs are no longer seen as the owner of all fraud risks within the health bodies. This will assist in fraud risks becoming truly embedded within the health bodies, with ownership resting with those individuals who can truly affect any mitigation that may be required at a local level.

These updates are available on the NHSCFA Extranet which is currently available to Local Counter Fraud Specialists and Directors of Finance.

Click here to access the full publication

Hackers target COVID-19 vaccine research

The Guardian have reported UK, US and Canadian organisations involved in researching and developing a vaccine for Coronavirus have been targeted by Russian state-sponsored hackers. The report comes following previous alerts and warnings to organisations involved in healthcare

and medical research, as the targeting of such organisations was predicted. The Guardian article references the NCSC, stating the group called APT29 is #almost certainly' part of the Russian intelligence service.
Read the full article here

Victims of coronavirus-related scams have lost over £11 million - Wednesday, 8 July, 2020
Action fraud has reported that a total of £11,316,266 has been reported lost by 2,866 victims of coronavirus-related scams. Action fraud has received 13,820 reports of coronavirus-related phishing emails.

Coronavirus: Man arrested over alleged £495,000 fraud of furlough scheme
We have previously reported in our alerts that HMRC have targeted those believed to have fraudulently claimed support under the governments furlough scheme. This week Sky News has reported that a 57-year-old man in the West Midlands has become the first person to be arrested in connection with an alleged fraud of the government furlough scheme.
HM Revenue and Customs (HMRC) said it had arrested a man from Solihull, on Wednesday, in connection to allegations of £495,000 fraud of the Coronavirus Job Retention Scheme. The report comes as the BBC report this week that the governments financial rescue schemes are set to lose billions of pounds to fraudulent claims.
Read the Sky News article here Read the BBC news article here

Calls for retired advisors to support police fight fraud
The Chartered Institute for Securities & Investment (CISI) has called on retired members to support the City of London Police fight fraud. Financial Times (FT) Advisor, a financial news website reports on the campaign by the CISI. The pilot campaign aims to support the fight against the rise in fraud during the coronavirus pandemic by asking retired members to volunteer and support the police to combat fraudsters.
Read the FT Advisor article here

Google report 18m phishing and malware emails per day
The Guardian has this week reported that Google has identified 18m malware and phishing messages, in addition to 240m COVID-19 related spam messages per day globally. The article states Google has identified a number of government backed attacker groups, using COVID-19 related content to target individuals. The report follows Google's submission to the Australian Senate Select Committee. We have recently reported in our alerts the Australian Prime Minister warned a range of organisations the country was facing sophisticated state backed cyber-attacks.
Read The Guardian article here

Two fraud arrests re: COVID-19 government business loans
Detectives from the Met's Economic Crime Unit have launched an investigation after two men were arrested for money laundering offences in Kensington.

Still in the early stages of investigation, the police believe the main suspect to have been recruiting individuals with the sole purpose of using their details to set up limited companies and bank accounts, which have then been used to launder money and facilitate fraud.
Read full article here

Nigerian serial fraudster and British partner lose more than £1million of assets

Over £1 million worth of assets have been recovered by the National Crime Agency (NCA) following a civil recovery investigation into a Nigerian fraudster and his long-term British partner, who both led extravagant lifestyles despite their combined declared annual income never exceeding £49,000.
Read full article here

COVID-19 pandemic linked to food fraud

Food Manufacture, a news publication for the food industry has this week reported that the COVID-19 pandemic may lead to the biggest case in fraud since the horsemeat scandal of 2013. The article states Lloyds Register, a food safety assurance specialist, has predicted the increase in food related fraud.
Read the Food Manufacture article here

National Cyber Security Centre (NCSC) provide businesses cyber resilience testing

The NCSC has provided a home and remote working exercise as part of the latest addition to the organisations Exercise in a Box Toolkit. The toolkit is aimed at helping small and medium sized businesses to carry out testing of its resilience and preparation for cyber-attacks.
Read more on the NCSC website here

Other type of fraud examples

Email scams & Phishing scams

- HSBC customers targeted in a new smishing scam. It begins with a text message purporting to come from HSBC, informing the victim that "a new payment has been made" through the HSBC app on their smartphone device. The victims are informed that if they were not responsible for this payment, they should visit a website to validate their bank account. The link – security.hsbc.confirm-systems.com then directs victims to a fake landing page (with HSBC branding) to input their username and password, along with a series of verification steps. Read more here
- Emails purporting to be from the Governments Driving Vehicle Licensing Agency (DVLA) suggest the recipients payment method has failed. Read the Which? article here
- Casino app Clubillion has experienced a database lead of millions of app users data. As leaked personal information is commonly used in phishing emails by cyber criminals, users of the gambling service are advised to be vigilant. Read further information from the NCSC

- Microsoft Office 365 users are now being targeted by a new phishing campaign using fake Zoom notifications warning their Zoom accounts have been suspended, with the end goal of stealing Office 365 logins. The phishing campaign has landed in over 50,000 mailboxes. The user may rush to click on the malicious link, and inadvertently enter credentials. Information likely be used later to facilitate identity theft and schemes such as Business Email Compromise (BEC) attacks. Read more here

Phone and Text Scams

- Action Fraud has received a report about fake calls made by fraudsters claiming to be the National Fraud Intelligence Bureau (NFIB). It should be noted that the NFIB will never contact you out of the blue to ask for your PIN, password or bank details.
- Cifas has warned of a premium rate number scams in operation - This scam tries to snare people who are searching online for telephone numbers of government advice services. It works by displaying an advert for the phone number of the relevant government advice line. However callers will be charged a premium for using this advertised telephone number – in some cases, as much as £20 or £30 a call. Searches for car tax discs, renewing your driving licence and completing tax your return are some of the areas currently prone to premium-rate number scams. Read the CIFAS article here
    - Never use numbers beginning with 084, 087, 090, 091 or 098 when calling government advice lines.
    - No official government service would ever use an 084, 087, 090, 091 or 098 number.
    - Use the official government services website to search directly for legitimate government telephone advice line numbers.

Social media and other messaging platforms

- Cifas has warned about scams about quizzes and links on social media: Due to COVID-19 and more people relying on social media sites, Cifas have seen new types of Facebook scams popping up more frequently. Most recent, a bait and switch scam – which uses a social media post to share fake links to viral videos. The link goes to a fake site with a virus which scammers use to steal personal and banking details. Similarly 'quizzes' and 'challenges' shared on social sites could pose a risk. A fellow social media user might innocently encourage their friends and acquaintances to share their personal information - which then gets into the wrong hands.
- Homeworkers are receiving bogus texts and emails claiming to be from Zoom, one message claiming to be from "Zoom Mail" informing the recipient that a "Zoom voicemail" has been received and that they should call a premium rate number, the message claims the cost is "£6 plus std net rate". Another message, sent via email, pretends to be a Zoom conference call invitation that asks the recipient to click a link to "review invitation". The link then leads to a fake login page which asks the recipient to put in their username and password, sending the information to scammers. Read more here
- Twitter accounts of well-known figures including Barack Obama, Kanye West and Elon Musk have been hacked in a crypto-currency scam. The hacked accounts are used to target individuals to donate financially using crypto-currency, with the promise of returning a

larger figure back to the individual. Read more here

In addition the National Cyber Security Centre (NCSC) has issued a statement on the Twitter attack. Read the NCSC statement here