COVID-19 Fraud & Security Alerts

Ref: CFMG-0013

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

NHS Supplier Warns of payment details change fraud

CMD LTD a manufacturer and distributor of ergonomics, power and electrical supplies, which provides goods to some NHS organisations, has warned clients of a fraudulent attempt to change its payment details with a customer. CMD LTD has directly contacted customers warning them to be aware of recent communications purporting to be from the company advising of revised payment details. The communication to registered customers asks that any organisation which has received similar contact regarding payment details to contact CMD LTD directly.

NHS prepares to implement Government Functional Standard

The NHS Counter Fraud Authority (CFA) has provided an update informing NHS providers and commissioners of the publication by the Cabinet Office of the Government Functional Standard GovS -13: Counter Fraud. The update also outlines the NHSCFA's plan to introduce the standard across the NHS detailing intended arrangements and timescales.

Access the update on the CFA Extranet here

NHS CFA kicks off new extranet project

The NHS CFA is starting a project to develop its current extranet function. As part of the development process the CFA will be sending out a short survey in August, with the aim of collating views of those who use the service. Following the survey a prototype will be created and tested. The CFA welcomes interest for members to joining the testing team, details of which can be found via the link below.

Read more about the project here

Anti-Corruption Strategy: year 2 update

HM Government has issued an update report covering the second year of the United Kingdom Anti-Corruption Strategy 2017-2022. The report shows that significant progress is continuing in the implementation of the strategies commitments. In addition it provides detailed descriptions of activity across the priority areas of the strategy.

Access the report here

National Fraud Initiative (NFI) Report

The latest version of the NFI Report has been published and is available online. The report is produced by the Cabinet Office and includes data matching with the aim of helping in the detection of fraud. The NFI is an exercise that matches electronic data within and between public and private sector bodies to prevent and detect fraud.

Read the 2020 NFI report here

Test and Trace programme unlawful, admits government

The Department of Health and Social Care (DHSC) failed in its legal obligation to complete a mandatory Data Protection Impact Assessment (DPIA) and has been operating unlawfully since its launch on 28 May 2020. The government was forced into the admission following a legal challenge from privacy campaigners at the Open Rights Group (ORG), who threatened to take it to court unless it agreed to immediately conduct one.

A DHSC spokesperson said: "There is no evidence of data being used unlawfully. NHS Test and Trace is committed to the highest ethical and data governance standards – collecting, using, and retaining data to fight the virus and save lives, while taking full account of all relevant legal obligations. We have rapidly created a large-scale test and trace system in response to this unprecedented pandemic. The programme is able to offer a test to anyone who needs one and trace the contacts of those who test positive, to stop the spread of the virus."

Computer Weekly understands that different elements of the programme have had DPIAs carried out, and that the DHSC is now trying to consolidate these, along with any additional analysis that may be relevant, into an assessment for the programme as a whole.

The Information Commissioner's Office's guidance state that organisations must complete a full DPIA if they plan to process data that 'is likely to result in a high risk to individuals', as any data related to people who have tested positive for Covid-19 may be.

Read full article here

Dussmann experience Ransomware data breach

German company Dussmann group, one of the largest private providers of facility management and care for the elderly have experienced a ransomware data breach. Info Security Magazine reports that the hackers have begun to post stolen files to the dark web. The group employs over 66.000 staff worldwide. The group behind the hack have posted 16,000 files as proof of the attack. Read the article here

Banks revel top Coronavirus scams

The BBC has this week reported the ten scams UK banks have warned the public to be wary of. The article outlines the UK Finance warning that scammers are using the pandemic and associated financial fears to scam members of the public. The article covers a range of scams including COVID-19 financial support, health and lockdown.

Read the BBC article here Read the UK Finance alert here

BBC Money Box podcast

BBC Radio 4's Money Box programme this week focused on fake emails, bogus calls and how to spot scams. The podcast is available on the BBC website. The episode includes real life stories, along with expert speakers such as police officers responsible for investigating frauds, and representatives from the finance industry.
Click here to listen to the podcast

Police warning as fraudsters make tax scam calls

Police are warning people of scammers claiming to be from HM Revenue and Customs (HMRC) tricking them into thinking they owe tax or debts and asking them to pay or purchase Google or Amazon gift cards.
Norfolk Constabulary has received three reports of victims being scammed by this method in Norfolk last week alone, with fraudsters trying to claim a total of over £12,000.
Read full details here

Four arrested as part of investigation into multi-million Tax phone scam

Financial Times (FT) Advisor, a financial news website, has this week reported that four individuals have been arrested following an investigation into a telephone scam which targeted UK taxpayers. An update from HMRC stated yesterday that two men and two women had been arrested and questioned for money laundering offences. The arrests follow previous warnings from HMRC outlining a range of scams relating to tax. Scams relating to tax have increased by 95% compared to the previous year's figures.
Read the article here

Inquiry into pension scams opened by UK Government

This week The Telegraph has reported that MPs have set out plans to open an inquiry into pension scams. During the pandemic reports of pension related fraud have more than doubled, as fraudsters target the financial concerns as a result of COVID-19. The article outlines that the first stage of a three part review, will identify the scams which have been used by fraudsters and how they can be prevented. The inquiry has been opened by the Work and Pensions committee with the aim of reviewing the impact of the pension freedoms introduced by the government in 2015.
Read the full article here

Other type of fraud examples

Email scams & Phishing scams

- Action Fraud has received over 1,000 reports about fake PayPal emails within 24 hours. The email states that the individuals account has been 'limited' as a result of policy violation. The links provided in the email lead to genuine-looking phishing websites that steal your PayPal login details and other personal information.

- Email users are being warned of a new phishing campaign, promising the recipient a government funded tax cut. The email appears to come from the 'Government Digital Service Team' stating, "You are getting a Council Tax Reduction considering you're on a low income or get benefits," "Total amount of benefits: GBP 385.50. The refunded amount will be transferred directly on your Debit/Credit card. Apply now to claim the reductions made over your past two years of Council Tax payments." The subject header states £385.55, one of several mistakes that would indicate the email is a scam. Always double check the source address of the sender and carefully examine the communication for typos and errors. Read more here
- South Lanarkshire Council has warned about a new Netflix scam, which could let you hackers access your bank accounts. A new email scam is in circulation, offering the chance to win a year's subscription to Netflix. The link leads to a login page, asking for your account and payment detail. Netflix have stated they will never ask for your personal or financial information over an email or text. Read more here
- Users of media streaming service Netflix have been warned to be aware of a phishing email scam. The email advises recipients of a promotion offering the chance to win a year's subscription. Links contained within the email require recipients to enter their account and payment details.
- Action Fraud has issued a warning to the public this week regarding a phishing attempt purporting to be from payment service PayPal. The warning follows over 1,000 reports within 24 hours to action fraud regarding the scam. The communication claims the recipients PayPal account has been 'limited' due to violating site polices. In order to reinstate the account, recipients are told to follow the links to a genuine looking bogus website, which aims to harvest log in details and other financial information. Read the Action Fraud warning here
- Consumer website Which? has this week circulated two guidance articles around holiday and motoring scams as part of its weekly scam alert service. The first article provides guidance on how to spot cams on letting sites such as Airbnb, whilst the second article provides guidance to consumers relating to scams purporting to be from the governments Driving and Vehicle and Licensing Agency. Read the holiday lettings article here Read the DVLA article here
- Info Security Magazine has reported a phishing scam purporting to be from supermarket retailer Tesco has been identified. The phishing emails and text messages along with fake social media pages claim the retailer have 500 TVs to give away, similar to previous scams seen purporting to be from electrical retailer Currys PC World. The latest scam aims to trick the public into handing over payment and confidential personal details. Read the Info Security Magazine article here

Malware

- The National Cyber Security Centre (NCSC) has issued a joint alert along with its US counterparts the Cybersecurity and Infrastructure Security Agency relating to Network Attached Storage device manufactured by QNAP. A legacy issue from a 2019 strain of malware may

leave QNAP devices vulnerable without the latest security updates. Read the NCSC joint alert here

Phone and Text Scams

- Gloucestershire Constabulary have been contacted by a number of residents who have received calls with an automated voice telling them that they owe tax, are going to be arrested or that their Amazon Prime subscription is about to renew. The victim is then encouraged to press one to speak to a member of staff. But these calls are said to be fake and the police want to spread the warning to not fall for it. Read more here

Websites

- The Insurance Business Magazine has reported this week that the Insurance Fraud Bureau (IBF) and City of London Police have issued a warning to the public to be aware of 'ghost brokers'. As a result of the COVID-19 pandemic and the financial concerns caused, the public may be more susceptible to scammers offering cheap vehicle insurance. The bureau warns that unless checks are made, drivers face the risk of buying invalid policies. The warning comes as a 25 year old man was arrested in May for 'ghost broking' by selling fake car insurance policies online. The scammer targeted NHS staff by offering discounts. Read the IBF guidance here Read the IBF article here Read the Insurance Business Magazine article here

Ransomware

- This week European law enforcement agency Europol has reported that a free tool has helped over four million visitors across 188 countries fight ransomware. The free scheme 'No More Ransom' helps users recover their stolen encrypted data without paying the ransom to criminals. It is reported the scheme has prevent $632m falling into criminal hands. Read the Europol article here