COVID-19 Fraud & Security Alerts

January 2021

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

Fake NHS vaccine messages sent in banking fraud scam

The BBC has reported that fraudsters are sending out bogus text messages about the coronavirus vaccine in an attempt to steal bank details. The scam informs the recipients that they are "eligible to apply for the vaccine" with a link to a bogus NHS website. That, in turn, asks for personal information and crucially bank details "for verification".

Read the full BBC article here

Man charged after administering fake COVID-19 vaccine, for £160, to an elderly woman in her home

David Chambers was arrested on Wednesday 13 January 2021 and taken to Bishopgate police station. He was charged on Thursday 14 January with two counts of fraud by false representation, one count of common assault and two breaches of COVID regulations. Remember, the vaccine is free of charge and at no point will you be asked to pay.

Read the full article here

Coronavirus vaccine scam warnings

Action Fraud has warned the public to remain vigilant as criminals begin to take full advantage of the roll out of the COVID-19 vaccine to commit fraud. As of January 7 2021 Action Fraud had received 57 reports in relation to the COVID-19 vaccine. Pauline Smith, head of Action Fraud, said: "The NHS will never ask you for details about your bank account or to pay for the vaccine. If you receive an email, text message or phone call purporting to be from the NHS and you are asked to provide financial details, this is a scam."

Read the full article here

Vaccine booking website criticised after 'queue-jumping' claims

Sky News have reported that an online system for booking COVID vaccine appointments has been criticised after claims ineligible people have been using it to "queue-jump" and receive the jab. The website is being used by numerous NHS Trusts to allow health and social care workers and over-70s to sign up for coronavirus vaccinations. However, links to the site's booking platform intended for NHS and care workers have

been posted on social media which has allowed those not yet eligible to book appointments.
Read the full Sky News article here

Group stole £320,000 from Worcester hospital in NHS fraud
Solomon Adeyemi, Emmanual Nbanga and his wife Remilekun Olusesi are accused of fleecing Worcestershire's hospitals of more than £322,000. They did not enter pleas to fraud, theft and money laundering against Worcestershire Acute Hospitals NHS Trust when they appeared before magistrates on 26 January 2021. This case involves the alleged theft of single use supplies from operating theatres which were then said to be sold back to the trust. The prosecutor told magistrates that the total value of the alleged theft and fraud was £322,482 made up of invoices paid by the trust, the value of invoices received for which no payment was made and the value of stock recovered during a search.
Read the full article here

Fraud epidemic is now a national security threat
Fraud has reached epidemic levels in the UK And should be seen as a national security issue, says think tank the Royal United Services Institute (RUSI). The scale of credit card, identity and cyber-fraud makes it the most prevalent crime reportedly costing up to £190billion a year. The Crime Survey for England and Wales found 3.7 million reported incidents in 2019-20 of members of the public being targeted by credit card, identity and cyber-fraud. The private sector takes the biggest financial losses; one estimate from 2017 put the cost of fraud to businesses at £140billion.
Read the full article here

Birmingham man sent scam vaccine texts pretending to be NHS
Munasar Jiniqow pleaded not guilty to charges of fraud by false representation and possession of blank NHS prescription slips for use in fraud at Birmingham Magistrates' Court on 21 January 2021. Jiniqow is alleged to have sent phishing and smishing messages purporting to be from the DVLA, HMRCS, Virgin and the NHS, intending to cause loss to unspecified persons between December 1 last year and January 21.
Read the full article here

Scam alert: Amazon gift card COVID19 email requests
Which? has reported that they often hear from scam victims who receive seemingly innocent emails from a friend, relative or work colleague only to discover that they were communicating with a fraudster all along. Once an email account has been hacked, criminals will try any way to make money; this includes sending emails to their contact list. A common tactic is to ask them to buy an Amazon gift card offering a spurious reason as to why they can't purchase it themselves, and the pandemic has given them the perfect excuse. As the recipients are likely to trust the address of the sender, they assume the request is genuine and agreed to purchase the gift cards. Now the scammer can simply ask you to share the serial numbers so that they can cash them in.
Read the full Which? article here

Scam Virgin Media telephone call

NHS staff have this month reported that they have received phone calls from a male stating that he works for Virgin Media and that there is a problem with the router. The individual then requested to take control of the staff member's computer before being questioned about the legitimacy of the call. The caller then ended the call.

Cyber criminals know that the NHS is busy

Nottinghamshire Health Informatics Service (NHIS) have released a security advice note detailing how techniques have been seen recently that include 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 including government organisations, banks and suppliers. Attacks also take place as phone calls. NHIS have recommended, to avoid systems becoming infected or individuals or organisations being compromised, colleagues should be vigilant and suspicious, never give out your own or anyone else's passwords, bank details or other sensitive data, check links in any password reset (or other) emails very carefully, don't open attachments, don't reply to spam or forward chain emails, change your passwords regularly and finally do not unsubscribe from any unsolicited spam emails as this confirms you are a real address.

Cambridgeshire man jailed after intercepting credit cards to go on a shopping spree

A man from Cambridge who committed over £60,000 of fraud has been sentenced to two years and six months in prison. Mr Waliu Jokosenumi, 32, pleaded guilty to committing fraud by false representation and being in possession of articles for use in fraud. This was following a successful investigation by the Dedicated Card and Payment Crime Unit (DCPCU), a specialist police unit funded by the banking and cards industry. Between April 2017 and December 2018, Mr Jokosenumi posed as genuine bank customers, submitting electronic applications for numerous credit cards in the victims' names. He then intercepted the credit cards in the post to go on a £60, 248 shopping spree at various retail and online stores.

Read the full article here

Police and Action Fraud warn public against cold call scammers

Police and Action Fraud have warned people against handing over money and valuables to scammers pretending to be police officers or bank officials. It comes after a number of "very distressing instances" involving resident in the West Yorkshire area. West Yorkshire Police and Action Fraud have said the scam begins when victims receive a cold call from a fraudster. The fraudster purports to be a police officer or bank official and then typically tells the victim to withdraw a sum of money to be collected by someone visiting their home address. Other versions of the scam include: fraudsters convincing the victim to transfer money to a "secure" bank account, handing over their bank cards, or high value items such as jewellery, watches and gold.

Read the full article here

Barclays not liable for couple defrauded of £700,000

The BBC has reported that a judge has ruled that a bank does not need to compensate a customer who was duped into paying £700,000 to

fraudsters. Fiona Philipp used her Barclays account to transfer two payments of £400,000 and £300,000 to an account in the United Arab Emirates. She and her husband thought that they were helping a high-profile fraud investigation being run by the Financial Conduct Authority (FCA). The scam started when her husband was called by a man who claimed to work for the CFA. He then told him that his bank, HSBC, and an investment company that he had savings in, were unsafe and at risk of fraud. In order to keep the money safe, the conman said it had to be transferred into "safe accounts" before his investigation could be completed.
Read the full BBC article here

Dental practice manager behind £60,000 fraud avoids jail
A Bupa dental practice manager who admitted a £60,000 fraud by paying 93 fake refunds into her own bank account has been spared jail. Jennifer Locke received a two-year suspended jail term and must do 250 hours unpaid work and obey a six months 9pm-6am curfew. The judge said Locke had been in a position of trust but he career as a dental nurse was over.
Read the full article here

Gambling addict financial director jailed for £800,000 fraud
A financial director who swindled her own firm out of over £800,000 to feed an online gambling addiction has been jailed for 32 months. Lauren Farr conned We Fight Any Claim for over three years whilst working for them as a senior executive. Farr used her own knowledge as a chartered accountant to hide the siphoning of the money from the company into her own bank account. The court heard that most of the money was spent on her gambling addiction but she also used the money to fund family holidays and a BMW X5 car.
Read the full article here

Experts warn against WhatsApp 'verification' scam that's currently being spread by hackers
A clever new WhatsApp scam is circulating and is hacking the accounts of those who fall for it. Thousands of unsuspecting users are being targeted by hackers with a message that makes you believe your account needs to be verified. The hacker will pose as one of your friends, saying they have accidentally sent you their authorisation code. However, this is all a ruse to get your own login code, which gives hackers access to your account, which means that they can text your contacts and read all of your messages.
Read the full article here

Residents get devices to protect them from fraud
State-of-the-art call blocking devices have been installed at homes in Knutsford and Alderly Edge to protect vulnerable residents from telephone scammers. Cheshire Police have stated that fraud is now the crime that citizens are most likely to fall victim to, with the force now dealing with more than 100 cases per week. Thanks to funding from the North West Regional Organised Crime Unit, these new devices will stop fraudsters in their tracks.
Read the full article here

Scam awareness training

Buckinghamshire and Surrey Trading Standards are pleased to offer 2 scam awareness sessions this February:

Friends Against Scams training session – 15th February 2021, 19:00 – 20:30, 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 – 16th February 2021, 19:00 – 20:30, 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 (https://www.friendsagainstscams.org.uk/elearning/surreybucks or attended one of our live Friends Against Scams sessions, such as the 15th February 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
Find out more about the scam awareness training here