COVID-19 Fraud & Security Alerts

Ref: CFMG-0017

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

Junior doctor facing disciplinary action after ' sophisticated' £7000 fraud

Dr Kristen Laing is appearing before a medical tribunal after attempting to claim £7,000 fraudulently for the theft of wedding and engagement rings. Dr Laing was working at Levenside Medical Practice in Dumbarton at the time of the incident and told insurers and police that her handbag had been taken. However, she had previously made a claim for the rings, on that occasion reporting that she had lost them.

Read full article here

Fraud warning as criminals hijack Government phone number

The UK Government has issued a warning after con artists hijacked an official number and are using it to try to scare people out of money. People are being told that if don't pay you could be arrested. A Government spokesman said: "We have been made aware that the Government Legal Department (GLD) general enquiry number (020 7210 8500) is being used by fraudsters to try and extract money from members of the public."

Read full article here

More than £38k stolen from HM Revenue and Customs (HMRC) scam victims in Hertfordshire

Fourteen elderly and vulnerable victims were contacted by the fraudsters claiming to be the HMRC over the last few weeks. The victims were targeted in Watford, Hatfield and Hertford and told that there were outstanding debts or unpaid taxes in their names and were then asked to make bank transfers as payment, resulting in a total loss of more than £38,000.

Read full article here

Pension savers claim over £30 million lost to scams as regulators urge footie fans to show scammers the red card

A new warning from the Financial Conduct Authority and the Pensions Regulator says that a total of £30,857,329 has been reportedly lost to pension scammers since 2017 according to complaints filed with Action Fraud.

The regulators recommend four simple steps to protect yourself from pension scams:

- Don’t be rushed or pressured into making any decision about your pension
- Reject unexpected pension offers whether made online, on social media or over the phone
- Check who you’re dealing with before changing your pension arrangements – check the Financial Services Register or call the FCA helpline on 0800 111 6768 to see if the firm you are dealing with is authorised by the FCA
- Consider getting impartial information and advice

Read full Action Fraud article here

HMRC investigates 10,000 Covid scams

HMRC is investigating 10,428 reports of phishing scams designed to exploit the coronavirus pandemic. Scams peaked in May after rising 337% from 133 in March to 5,152 in May. They subsequently fell as lockdown measures began to ease, with 2,558 incidents reported in June, involving email, SMS, social media, and phone scams.

Read full article here

Brits shunning cash due to fear of Covid spread

Research commissioned by GoCompare Money found that a third of UK adults are avoiding using cash because of the risk of spreading coronavirus. Contactless payments are now the preferred way of paying for many people and the fear of fraud remains a big issue for some. Lee Griffin, CEO and founder of GoCompare, said: “In early March, there were news reports about the spread of the coronavirus on banknotes and coins. However, the Bank of England and the World Health Organization have stressed that cash doesn’t pose any greater risk than any other items and, repeated the advice on regular hand washing. However, from the results of our survey, it’s clear that many people remain concerned about the potential of money to be contaminated. With a lot of people using contactless and online payments for the first time and millions of us relying on them, it’s more important than ever to keep on top of your finances by checking your bank and card statements. Regularly checking though your statements will help you keep abreast of your incomings and outgoings and help you spot whether any payments have been fraudulently taken.”

Read full article here

Woman sentenced for fraudulently claiming benefits for relatives

Saaba Mahmood, from Stockport, fraudulently claimed £95,000 in benefits by acting as an appointee for her aunt, her uncle and her mother who were claiming benefits. She was sentenced to 16 months in prison, suspended for 18 months. She must do 15 days of a rehabilitation activity and 150 hours of unpaid work in the community.

Read CPS article here

Firewall best practices to block ransomware

Ransomware continues to plague organizations, with over half of companies surveyed across 26 countries revealing that they were hit by

ransomware in the last year. Such attacks are ever increasing in complexity and are getting more efficient at exploiting network and system vulnerabilities, leaving organizations with a significant clean-up bill. Modern firewalls are highly effective at defending against these types of attacks, but they need to be given the chance to do their job. This whitepaper discusses how these attacks work, how they can be stopped, and best practices for configuring your firewall and network to give you the best protection possible. The paper covers: Who hackers are targeting; How to stay protected from ransomware; and Best practices for firewall and network configuration.
Read publication here

One of the biggest online piracy groups in the world taken down

On 25 August, an alleged criminal network of copyright infringing hackers, mainly responsible for pirating movies and hosting illegal digital content worldwide was dismantled in a coordinated action between US authorities and their counterparts in 18 countries around the world, with Europol and Eurojust support. Sixty servers were taken down in North America, Europe and Asia and several of the main suspects were arrested.
Read full article here

Other type of fraud examples

Email scams & Phishing scams

- Action Fraud have had over 150 reports about fake tax refund emails within 24 hours. The email claim to be from government departments, including HRMC. The emails state that the recipient has 'an outstanding tax refund' that they need to claim urgently. The links in the email lead to genuine-looking phishing websites that are designed to steal personal and financial details. Remember the bank or any other official organisation won't ask you to share any personal details over email or text. If you need to check call the organisation directly.
- Beware of any email or text from HMRC asking you to provide personal or financial information. HMRC would never ask you to disclose personal or financial information via email or text.
- Fake TV licensing emails are still doing the rounds. The convincing looking email contains links to websites designed to steal personal and financial details. Don't click on the links or attachments in suspicious emails and never reply to requests for personal and financial info. Read more here

Social Media

- Romance fraud continues to be an issue with more than £175,000 stolen from Scots. Police have issued a warning over scammers who create fake profiles on dating sites and social media apps. Read more here

Phone

- The Chartered Trading Standards Institute (CTSI) has received intelligence on a scam involving callers pretending to be from a bank security team. CTSI Lead Officer, Katherine Hart, said: "These types of scams attempt to reassure the target by 'spoofing' the telephone number of their bank when calling. Bank security teams will never ask you to send money to any account. If you have concerns then you should call your bank directly – do not rely on them to call you as any number can be easily spoofed on caller ID." Read full article here
- Scammers are calling victims, posing as workers from Microsoft and claim to be computer security engineers, telling residents their computers are at a security risk. They say a security check needs to be performed and if the victim agrees, the scammers then gain remote access to the computer, which allows them to obtain personal details, including bank account information.

Other

- TSB is also warning over emerging green deal scams where criminals promise to install energy efficient equipment, like solar panels, part funded by a government grant; but instead scam the victims with an average loss of £7,500.