COVID-19 Fraud & Security Alerts

September 2020

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

NHS supplier mandate fraud attempts

We have been alerted that a NHS supplier has warned customers of a mandate fraud attempt. Plans4Rehab, a community provider of specialist care in Leicester, has reported a security breach regarding one of its email addresses (accounts@healthcaremanagementuk.com). Fraudulent emails have been sent to customers claiming that their bank details have changed. Plans4Rehab have confirmed that their invoices would include the correct bank details and any emails in regards to the changing of bank details should be ignored and forwarded to them for review.

Automated phone call warning

An NHS Trust has received several automated phone calls warning that the internet will be disconnected unless they press "1". Calls like this are attempted frauds. How this usually works is if the call receiver does press a number, they will be connected to a person who will then try to extract personal details which they can use to commit offences, or they will pressure the call receiver to take actions which will allow them remote access to the computer systems. Another trick which can be used is to connect the call to a premium rate number then keep the victim hanging on the line in order to rack up a small fortune.

You may receive calls like this to your home phones as well as through hospital phones.

If you receive such as call:

- Hang up immediately.
- Do not speak.
- Do not press 1 (or any other key on the phone).
- Never give out information or answer any questions.
- Do not verify the call by using any information given during the call.

If you do wish to make further enquiries, use a different phone, or wait at least 20 minutes before using the same phone (in case the original fraudster is still controlling the line).

Fraud Advisory Panel

The Fraud Advisory Panel latest updates on 3 September and 17 September 2020 includes; 'current COVID19 fraud risks', most of which we have covered in our weekly alerts; 'Anticipated and/or emerging issues'; and 'some simple preventative tips', with links to some useful documents and contacts.

Read more here

BBC warns of Test and Protect phone scam

The BBC has warned of the continuing scams relating to COVID-19 track and trace and testing schemes. Residents in Scotland have been targeted by cold-callers claiming to be from the governments Test and Protect tracing service. During the calls victims are asked to pay £500 for a test. Following warnings of the scam First Minister Nicola Sturgeon has confirmed Test and Protect staff will never require financial information or require payments for testing.

Read the BBC article here

COVID-19 fraud: be on the lookout and act fast

On 7 September 2020 the Institute of Chartered Accountants in England and Wales (ICAEW) reported that Initial estimates have found that coronavirus-related fraud could end up costing the taxpayer £4bn.

Read full article here

What is Sharenting? How you could be putting your child's identity at risk online

Parents have been warned they could be at risk of identity theft and online fraud by 'sharenting' on social media. The term 'Sharenting' is when parents post personal information about their children on social media. This information could later be used by fraudsters. According to security specialists from Barclays bank, it has never been easier for identity thieves to find targets, as a child's information will remain online indefinitely. By 2030, sharenting could cost close to £670 million in online fraud per year, according to Barclays.

Read article here

Bank branch staff and police team up to stop £19 million of fraud in first half of 2020

Bank branch staff worked with the police to stop £19 million of fraud in the first half of 2020 through the Banking Protocol, a scheme that alerts local police to suspected scams. Since the scheme was introduced three years ago, it has prevented victims from losing £116 million of fraud and led to 744 arrests

Read Action Fraud article here

Mitigating malware and ransomware attacks

This guidance has been updated 11 September 2020 ad will help private and public sector organisations deal with the effects of malware (which includes ransomware). It provides actions to help organisations prevent a malware infection, and also steps to take if you're already infected.

Following this guidance will reduce:

- The likelihood of becoming infected
- The spread of malware throughout your organisation
- The impact of the infection

Click here for updated NCSC guidance

Three former G4S executives charged with fraud against taxpayer

The Serious Fraud Office has charged three former executives of G4S Care and Justice Services (UK) Ltd (G4S C&J) with multiple offences in relation to a multi-year scheme to defraud the Ministry of Justice (MoJ). They have each been charged with seven offences of fraud in connection to false representations made to the MoJ between 2009 and 2012.

Read article here

Fraudulent foreign exchange trader pleads guilty to a £20.5million investment scam

A fraudulent foreign exchange trader has today pleaded guilty to a £20.5million Ponzi international investment scam. Based in Turkey, Joseph Lewis, 65, attracted clients across the globe to invest in Foreign Exchange Trading, when actually it was a scam. The Ponzi scheme he had been running for the past decade and told them how he'd taken millions from people who thought they were investing in foreign exchange trading.

Read CPS article here

Cyber security alert issued following rising attacks on UK academia

The National Cyber Security Centre (NCSC) has issued an alert to the academic sector following a spate of online attacks against UK schools, colleges and universities. The alert contains a number of steps they can take to keep cyber criminals out of their networks, following a recent spike in ransomware attacks.

Read NCSC article here

UK condemns Chinese cyber attacks against governments and businesses

The UK has joined international allies to call out malicious cyber activity carried out by China. The Foreign Secretary, Dominic Raab, said:

"Today we have another example of the Chinese using malicious cyber activity for criminal ends. We condemn the attempted attacks against governments and businesses. This kind of opportunistic and reckless behaviour in cyberspace is wholly unacceptable.

"The UK will continue to counter those conducting such cyber-attacks, and work with our allies to hold perpetrators to account."

Read full NCSC article here

UK Finance report increase in impersonation scams

UK Finance has reported that impersonation scams reported in the first half of 2020 show an increase of 84% compared to the same period last year. Figures show that £58m has been lost to the fraud in the first six months of the year, with almost 15,000 reported cases. UK Finance

define an impersonation scam as a scam in which the victim is persuaded to make a payment to a criminal claiming to be from a trusted individual or from a reputable organisation such as bank, utility company, police force or government department.
Read the UK Finance article here

BBC reports up to £3.5bn furlough claims fraudulent or paid in error

The BBC have reported that up to £3.5bn has been paid out in error or to fraudulent claims following a meeting of the Public Accounts Committee in which representatives from HMRC estimates between 5 to 10% of furlough payments have been awarded in error. The Financial Times have also reported that HMRC would focus on addressing furlough related fraud. HMRC have confirmed that it would be writing to employers in order to give them the opportunity to rectify claims made in error and repay the payments made by HMRC. The article also confirmed that the HMRC reporting line for furlough fraud had received 8,000 calls whilst it was investigating 27,000 claims deemed high risk.
Read the BBC article here Read the Financial Times article here

American consumers lose $145m to COVID-19 scams

The New York Times have reported that over 200,000 complaints of scams have been reported to the Federal Trade Commission, which total in excess of $145m. Data shows that the average loss stood at $300, whilst this increased for older victims. A range of scams have circulated across America, with many parallels to those seen in the UK.
Read the New York Times article here

New COVID-19 tactics to rip off consumers

The annual National Trading Standards Harm Report reveals how criminals are adapting to changing consumer and business needs as the coronavirus pandemic develops. While the immediate issues exploited by criminals earlier this year involved the fraudulent sale of fake PPE, hand sanitiser and testing kits, emerging and future issues are likely to include:

- Price gouging from profiteering traders as demand for specific products rises rapidly
- Online fraud
- Legitimate government initiatives that are exploited by criminals
- New websites and social media accounts offering 'miracle cures'
- Virtual home viewings that misrepresent the property for sale or let.
- Fake refund websites
- Exploiting the vulnerable is not a new tactic – but we expect it to become more prominent

More information is provided in the 2020 Consumer Harm Report, available here.
Read full article here
The Telegraph has recently cited the report in an article focusing on COVID-19 testing scams. Read the Telegraph article here

Upcoming Friends Against Scams Sessions

In association with National Trading Standards, Friends Against Scams have developed online 'scam champion' training sessions, which aim to make participants aware of scams and how to avoid then. Friends Against Scams have now developed a training session for those wishing to deliver the session within their communities and organisations. The train the trainer sessions will run on 1 or 6 October, click here for further details. In order to attend the session users are required to complete the Friends Against Scams E-Learning which can be accessed here.

The Metropolitan Police have released five very short fraud awareness videos a on: Test and Trace; Phishing; Working from Home; Vishing and; Ransomware

Most last less than a minute and provide clear advice to help you protect yourself against fraud.

Click here for the fraud awareness videos

Are you or your loved ones being targeted by scams?

A guide has been prepared by the National Trading Standards Scams Team and the National Centre for Post Qualifying Social Work and Professional Practice at Bournemouth University, working in partnership with Lloyds Bank, Halifax and Bank of Scotland.

This guide provides information to individuals and their loved ones to help protect them from scams. It suggests measures that can be put in place to help prevent criminals from making contact, such as the use of call blockers and the mail redirection service. It also provides information on managing finances to reduce the risk of scams, such as implementing a Lasting Power of Attorney.

Click to read guide

Criminals exploit COVID-19 as fraud moves increasingly online

Figures from UK Finance's 2020 half year fraud update report have revealed that losses to unauthorised fraud fell by eight per cent in the first half of this year to £374.3 million.

UK Finance is warning that criminals have been exploiting and adapting to COVID-19 with a growth in fraud and scams that target people online. There is often a delay between criminals obtaining people's details and using them to commit fraud, meaning the full losses from COVID-19 related scams in the first half of this year are likely to not yet have been fully realised. Key headlines include:

- Unauthorised fraud fell by eight per cent to £374.3 million in first half of 2020, as the banking industry prevented £853 million of losses.
- Criminals are exploiting and adapting to Covid-19 with a rise in online data harvesting and a fall in cheque and contactless card fraud.
- £207.8 million was lost to Authorised Push Payment (APP) fraud, in line with the same period last year. Finance providers were able to return £73.1 million of APP fraud losses to victims, up 86 per cent compared to last year.
- £47.9 million of losses were reimbursed to victims under APP voluntary Code in first half of 2020. UK Finance is calling for legislation to ensure greater consistency for customers.

Read UK Finance article here

Other type of fraud examples

Online & Email scams

- Action Fraud has received over 1,000 reports in 24 hours about FAKE penalty charge emails. The Fake emails are claiming to be from HM Courts and Tribunal Service. The email states that the recipient has been issued a penalty charge for 'the use if a vehicle on a road in the charging area which a charging scheme applies without payment of the appropriate charge'. The links in the emails lead to genuine looking phishing websites that are designed to steal your personal and financial details.
- Consumer champion Which? has recently warned the public of scam adverts that appear in Google search results. Scammers are using search engine advertisements in an attempt to appear genuine. Research by Which? found an array of adverts which sit above genuine search results spanning the financial services sector. In one case, a victim was duped into investing £160,000 in fake bonds. Which? has also produced a podcast focusing on this area of increasing fraud. The Guardian has produced an article on the scam following the press release from Which? Read the full report by Which? here Access the Which? podcast here Read The Guardian article here
- Phishing emails purporting to be from the Governments Driving and Vehicle Licensing Agency continue to circulate and be reported. The email communication claims to require the user to update their personal details and financial information. The communication may appear genuine with statements regarding the security of data protected and similar branding and styling to usual DVLA emails. Communications have recently warned victims that their driving licence may be revoked if the data is not provided. The DVLA have confirmed that they will never ask users to reply with personal or bank details.
- The Student Loans Company (SLC) have warned of phishing scams as the university term begins and student loan payments start. SLC has warned students that scammers may target students around the three payment dates (September, January and April) with emails or text messages. Communications may purport to be from the SLC to confirm bank details. Guidance from SLC provides details of how to spot scams and can be accessed here.
- Business Matters Magazine has reported a new phishing email circulating which is targeting business owners. The communication purporting to be from HMRC advises recipients that their claim to defer VAT payments as part of the COVID-19 support package has been rejected. The communication requires the victim to provide personal and fiancé details to review the outcome of the decision. These details may then be used by fraudsters for a range of fraudulent activity. Read the article here.
- A phishing email purporting to be from energy supplier British Gas has been identified. The communication informs recipients their account is in debt and contains a link to log in and pay. This has been confirmed as a scam email and is an attempt for fraudsters to gain personal and financial information. Read more here

Other

- Another scam in circulation is the Gold Courier Fraud. Courier fraud is when criminals impersonate an otherwise respectable organisation, such as a bank or police constabulary, in order to convince victims to hand over cash, bank cards or high value items to courier's sent to the victim's house. In the last three months Action Fraud has received 13 reports with losses totalling almost £419,000, where the criminals instruct unsuspecting victims to purchase high value items such as gold coins and gold bullion. Remember, your bank or the police will never:
  - Ask you to verify your personal details or PIN by phone or offer to pick up your card by courier.
  - Contact you out of the blue to participate in an investigation in which you need to withdraw money from the bank or purchase high value goods.
  - Send a courier to your home to collect your card, PIN, or other valuables.