COVID-19 Fraud & Security Alerts

November 2020

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

COVID: Hertfordshire firm sues as £45m NHS masks deal collapses

Five million medical masks bought by the government for £45m are missing amid claims of fraud. The respirator masks were due to arrive in the UK by June, but the company could not supply them.

Hertfordshire-based Purple Surgical has filed papers alleging fraud by its supplier Win Billion Investment Group, a firm in the British Virgin Islands, as first reported in the Guardian .

Read BBC article here

Benefit scams worth £1bn foiled during lockdown

The BBC has reported that fraudulent benefit claims totalling up to £1bn have been prevented during the COVID-19 pandemic. Civil servants identified in May numerous claims for Universal Credit requesting payments were made to the same bank account. Upon further investigation staff identified over 100,000 fraudulent claims. The article by the BBC also reports that officials had confirmed personal details for thousands of members of the public with the scammers. The article states that although the Department for Work and Pensions plan to write to those compromised, it is struggling to identify many of them.

Read the BBC article here

73% increase in phishing attacks reported to HMRC

Info Security Magazine reports that HMRC detected a 73% rise in phishing attacks during the first six months of the COVID-19 pandemic. During the two months prior to COVID-19 lockdown restrictions the average email attacks were 26,100. This rose to an average of 45,046 during March and September, amounting to a total of 367,528 reports of phishing attacks in 2020 up to September. The article also reports that whilst almost a further 200,000 phone cams and 59,000 SMS scams were reported, these scams were at the lowest point in April. It is believed that this could show in the first month of lockdown fraudsters focused on email phasing attacks to take advantage of home working.

Read the Info Security Magazine article here Read the Which? guide to spotting phishing scams

Can you spot the COVID-19 scams?

Financial news website This Is Money has produced an article raising awareness of a number of scams currently circulating. The article includes examples of communications used to trick the public including for Netflix, the Environment Agency, UK Government, TV Licencing and Amazon. UK Finance's managing director of economic crime, Katy Worobec, said: 'Criminals are cynically preying on those with financial concerns at this time of national crisis. They are experts at impersonating other organisations, whether it's your bank, the police, a mobile phone network or a government department. Criminals might spend weeks researching you but they only need you to let your guard down for a minute. Everything they do is designed to make them sound genuine and convince you to make a payment or give away your personal and financial details. It's important not to let the criminals rush or panic you into making a decision that you later come to regret. If you do receive a call, text message or email, don't be afraid to refuse, reject or ignore their request.'

Read the full article here

Google identified 2 million phishing sites in 2020

A recent article by American business magazine Forbes has identified that so far in 2020 Google has identified 2.02 million phishing websites. The figure represents an almost 20% increase compared to the full figures for 2019. The article highlights the impact of the COVID-19 pandemic and the increased opportunities created for online scams. The article reviews the current trends in phishing, highlighting that whilst the increase is part of a historic trend, the COVID-19 pandemic has accelerated it.

Read the full report by Forbes here

Action Fraud launches new campaign to fight back against fraud this Christmas

Action Fraud's #FraudFreeXmas campaign has launched, with a warning about 'too good to be true' Black Friday deals. Figures reveal reports of online shopping fraud have surged by 30% over the pandemic as many of us continue to shop online in light of current restrictions.

Remember the following to protect yourself from falling victim to online shopping or auction fraud:

- choosing where you shop
- payment method
- staying secure online
- watch out for phishing emails or texts
- when things go wrong.

Read full article here

Fake PayPal emails lead to nearly £8 million in losses this year

Between January 2020 and September 2020, 21,349 crime reports, with losses totalling £7,891,077.44, were made to Action Fraud about fake PayPal emails.

Criminals have been targeting people selling items online, by sending them emails purporting to be from PayPal. The emails trick victims into believing they have received payment for the items they're selling on the platform.
Generally, after receiving these emails, victims will then send the item to the criminal. This leaves them at a further disadvantage having not received any payment for the item and also no longer being in possession of it.
Read Action Fraud article here

Action Fraud warns of rise in investment fraud reports as nation enters second lockdown
Between September 2019 and September 2020, Action Fraud received just over 17,000 reports of investment fraud, amounting to £657.4m in reported losses, which is a 28% increase compared to the same period last year. Reports spiked during May to September 2020 as the nation adjusted to life after lockdown.
How to protect yourself from investment fraud

- be suspicious
- don't be rushed into making an investment
- seek advice
- use a financial advisor accredited by the Financial Conduct Authority
- Use the Financial Conduct Authority's register
- Just because a company has a glossy website and glowing reviews from 'high net worth' investors does not mean it is genuine
- Remember, if something sounds too good to be true, it probably is.

Read article here

Black Friday shoppers urged to avoid handing cyber criminals early Christmas gift
The National Cyber Security Centre (NCSC) has updated guidance ahead of Black Friday to help people shop online securely. Online shoppers searching for Black Friday bargains are being encouraged to follow NCSC top tips to stay safe contained in the shopping online securely guidance and prevent cyber criminals cashing in on the annual sales rush.
Read NCSC article here

Specialist prosecutors bring major investment scammers to justice
Through its dedicated Specialist Fraud Division, the Crown Prosecution Service (CPS0 is cracking down on these terrible crimes which often result in a large financial loss to victims who have in good faith invested their savings and pensions. Head of the Specialist Fraud Division at the CPS, Andrew Penhale, said: "*The harm caused by these fraudsters is immense - stripping individual victims of their savings, raiding pension pots and wrecking their futures."*
Since the end of September CPS have brought three major investment scammers to justice: David Stevens, 67, carried out a five-year

investment scam resulting in a loss of £1,200,000 to his victims; Joseph Lewis, 65, ran a £20million Ponzi scheme fraud for a decade, taking millions from people who thought they were investing in foreign exchange trading; Freddy David from Elstree was found to have run a Ponzi scheme fraud between 19 December 2004 and 9 November 2017.
Read CPS article here

Officers foil fraudsters from stealing €40 million in payment card scam
Carding Action 2020, an operation led by law enforcement agencies from Italy and Hungary and supported by the UK and Europol, targeted fraudsters selling and purchasing compromised card details on websites selling stolen credit card data, known as card shops, and dark web marketplaces. During a three-month operation, 90,000 pieces of card data were analysed preventing approximately €40 million in losses.
Read Europol article here

Covid-19 chiefs of police working group: fighting the pandemic and criminals together
European chiefs of police from Austria, Belgium, France, Germany, Italy, the Netherlands, Poland, Spain, Switzerland, the United Kingdom and Interpol came together to discuss the topics surrounding criminality and COVID-19. Topics were discussed and the following areas were identified as a priority for the working group:

- given the increased online presence of individuals, there have been growing concerns of potential scams and attacks, notably, surrounding fraud related to health products
- some Member States saw a significant increase in online child sexual exploitation material. In some countries the statistics of the distribution of images and explicit videos indicated that it had become six times more frequent
- the need to identify and monitor indicators related to the infiltration of organised criminal groups into the legal economy.

Read Europol article here

How COVID-19-related crime infected Europe during 2020
While the COVID-19 pandemic is first and foremost a global public health crisis, it has also proven to have a significant and potentially long-lasting impact on the serious and organised crime and terrorism landscape in Europe as well as the ability of Member State law enforcement authorities to counter security threats. See the Europol report on How COVID-19-related crime infected Europe during 2020

Apple's security chief charged with bribery
Apple's head of global security has been charged with bribery. He has been accused of offering bribes in the form of iPads worth $70,000 in order to obtain concealed firearms licenses.
Read BBC article here

Woman guilty of fake cancer GoFundMe fundraising fraud
A woman who faked a cancer diagnosis to claim more than £45,000, by setting up an online fundraising campaign, has been convicted of fraud.

Police began an investigation after a doctor, who had recently given her the all-clear, raised suspicions.
Read BBC article here

More than £60,000 taken from people in lottery scam in West Midlands

At least 10 residents have been conned out of more than £63,000 in the region over the past three months, police have said. Scammers phone their victims and say they have won a UK or international lottery and trick people into believing it's true. Winners are asked to keep winnings a secret and asked for payment to cover taxes to ensure the victim can collect their cash prize.
Read full details here

Friends Against Scams Training Sessions

Buckinghamshire and Surrey Trading Standards are pleased to offer some upcoming free virtual scam session. The sessions have been offered in previous months and have received positive feedback. The courses aim to increase the knowledge of attendees on the subject of scams. The sessions are as follows;

- Friends Against Scams training session – 3rd December, 15:00 – 16:30, 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.
- ScamChampion training session – 8th December, 14:00 – 16:00, 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 (http://www.friendsagainstscams.org.uk/elearning/surreybucks) or attended one of our live Friends Against Scams sessions, such as the 3rd December course.

Please email natalie1.webb@surreycc.gov.uk to confirm attendance on each/either course

Other type of fraud examples

Online & Email scams

- A range of health and medical scams have been identified recently. Commonly, scammers use fake advertisements and emails to trick members of the public with offers of miracle cures. Action Fraud have provided the following guidance:
    - Proceed with real caution when considering any new medicine or health care product
    - Avoid payments by money transfers, as they are not secure
    - Do not send confidential personal or financial information

- Check the pharmacist's registration status.

- Action Fraud have warned of the dangers of phishing emails, which attempt to trick people into 'doing the wrong thing'. As information from websites and social media accounts can be exploited, Action Fraud has issued the following guidance:
  - Review your privacy settings
  - Be aware what your friends, family and colleagues say about you online
  - If you spot a suspicious email, flag it as spam/junk in your email inbox and report it to Action Fraud.
- As online retailers have seen a surge in sales as a result of national lockdowns and Black Friday sales, consumer organisation Which? has produced an article covering how to spot online scams. The article covers scam social media posts, scam search engine advertisements and general hints and tips such as browsing the web and doing your research before buying. Click here to access the article.
- A scam email purporting to be from Microsoft has been identified in recent weeks. The email claims that the recipient is entitled to a payment from a relief fund to support Microsoft users around the world during the COVID-19 pandemic. Users are told to visit a genuine looking webpage to enter personal details. Read the full report here
- Royal mail post scam targets Liverpool and Hull residents - There has been a reported spike in fraudsters sending out unsolicited emails to residents in Liverpool and Hull purporting to be from the Royal Mail. They ask that residents pay a £1.99 'redelivery fee' for a letter they were 'unable' to post through the mailbox. Cifas advises residents to: Check the sender's email address as they may contain an extra letter, number or full stop; Check the spelling and grammar of the emails as errors are often indicative of a scam.

Calls and messaging services

- We have previously reported that scam calls purporting to be from online retailer Amazon attempt to trick the public by claiming to confirm an unwanted Amazon Prime subscription. The automated calls tells the recipient that their Amazon subscription will be renewed at a cost of £39.99, stating those who wish to speak to an account manager should press one. The fraudulent account managers attempt to steal personal and financial information. Read the Which? warning here
- Phone scam targets Cumbria residents - Fraudsters are cold calling Cumbria residents, claiming that they are going to 'receive' a sum of money. They provide a code and claim that a 'cheque' will be delivered to their home. In order to 'release' the funds, residents are urged to purchase a gift card from their local shop. Cifas advises residents to be suspicious when receiving an unsolicited call and to avoid handing over bank details or PIN numbers over the phone. Cifas reminds residents that no reputable organisation would ask for payment of a bill or debt using vouchers or gift cards.

Social Media

- Facebook Secret Santa pyramid scheme alert - There is a Secret Santa themed pyramid scheme scam currently circulating on Facebook. The scam also known as the 'Secret Sister Gift Exchange' is organised through Facebook groups and encourages recipients to send a low-value gift to another individual from a long list of participants. It 'promises' 36 'gifts' from strangers in return. Cifas advises Facebook users to: Be wary of opportunities that promise a huge return on a small initial investment; Check the legitimacy of an investment opportunity by taking the FCA's ScamSmart test; Avoid sharing personal details such as your address on social media. Read the article here
- Scottish government Test and Protect scam alert - Fraudsters are sending out fake text messages to residents in Scotland claiming to be from Scotland's Test and Protect program. They claim that recipients have come into contact with someone who has tested positive for COVID-19. The latest version of the scam is circulating via WhatsApp and urges recipients to reply to an unknown number with personal details. A genuine contact tracer will never ask for personal details such as medical records or banking details. Read more
- Fake £35 ASDA voucher scam alert - ASDA shoppers warned of a potential scam that is circulating on Facebook promising free ASDA vouchers. The scam is featured on a fake page called 'ASDA Stores', where fraudsters claim they are giving away a gift box that contains a '£35 ASDA vouchers' to celebrate ASDA's 71st Anniversary. Users are directed to a malicious link that asks for their email address, bank details, phone number and security code. This scam is an attempt to steal confidential data and shoppers should avoid clicking on links and avoid parting with personal or banking details. Read more

Other

- Recent lockdown restrictions have caused an increase in reports of door to door salesman. Which? has reported on the subject with a 6 minute guide covering a general overview and statistics as well as top tips, what to do if you're caught out and example of common door step scams. Read the Which 6 minute guide here
- Customers of Starling bank who use Android devices and some older Apple users who have not updated the Starling app have been urged to check their accounts. For 31 days from 12 October 2020 users may not have received Confirmation of Payee warnings. These warnings are designed to highlight when the name doesn't match the account details when transferring money. Starling bank has confirmed that users will be required to update the app the next time they set up a new payee. Read the full report here