COVID-19 Fraud & Security Alerts

October 2020

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

Fraud Awareness Month

November is Fraud Awareness Month (FAM). Over the next few weeks you will see a whole range of materials being published to tell you about how fraud, bribery or corruption could affect the NHS, or you in your home life, and what you can do to protect yourself.

Ordinarily, FAM involves sight visits, presentations and face-to-face discussions with healthcare staff across the East Midlands. This year, given the restrictions we are all living under, FAM is being held virtually.

There'll be a newsletter, posters, the Ultimate Guide to Cyber Crime, role-specific aide memoirs and other awareness raising information sent out throughout the month.

We'll also be holding a drop-in session via Microsoft Teams throughout 24th October 2020. To join the session, just use this link.

For now, read on to find out about the latest fraud, scams and related information that have been identified and published in the last month.

COVID Crimestoppers hotline launched

A new anonymous reporting line has been set up by the government for the public to report suspected fraudulent claims for government backed COVID emergency business loans. The hotline, in partnership with Crimestoppers, allows the public to report those organisations believed to have made fraudulent claims against the emergency loan and grant schemes offered to UK business. The Guardian reports that the government has been recently criticised for failing to act on expert warnings about the schemes, which allow small businesses to quickly claim up to £50,000. Recent warnings have come from the National Audit Office and National Crime Agency regarding the business loans, it is thought that the UK government could stand to lose a figure of billions of pounds to false claims. It is reported that the hotline will operate for 12 months, at a cost of £100,000. The hotline will not take calls relating to other fraudulent claims of government support such as furlough or 'eat out to help out' schemes, as these are directed to HMRC.

Read The Guardian article here Read the UK Governments press release here

Friends Against Scams publication

The National Trading Standards Scams Team, along with other partners, has produced a scam guide with a range of information to prevent

people falling victims of scams. The publication contains measures that can be put in place to prevent criminals from making contact, as well as information on managing finances to reduce the risk of scams. The guide is aimed at those most vulnerable of falling victim to scams and their families.

Access the Friends Against Scams guide here

Action Fraud warns charities and public to be vigilant

This month the Charity Commission has warned both trustees and donors to strengthen defences fearing a rise in charity fraud as a result of the pandemic. The warning comes as we enter Charity Fraud Awareness week which runs from 19 to 23 October. Action Fraud have reported that since March, 645 cases of charity fraud have been reported, amounting to a loss of £3.6 million. The Charity Commission has warned that remote working has resulted in virtual actives and sign off processes may make them vulnerable. The commission warns that those charities providing support in the community may be at risk of being victims to PPE scams. A recent fraud warning from Greater Manchester Police and Action Fraud highlighted the three top fraud threats from charities are ransomeware, money transfer and push-payment scams.

Helen Stephenson CBG, Chief Executive of the Charity Commission said 'We are seeing evidence that opportunists may be taking advantage of charities during the pandemic and I urge all charities to be extra vigilant against fraud. This comes at a time when charities are a lifeline for many people suffering from Covid-19, and the wider impacts of the pandemic - charities have been at the forefront of responding to the crisis, and many have also been placed under severe financial strain. As our country faces another challenging point in the crisis, we cannot afford for charitable work to be disrupted by criminals. When fraud hits charities, its impact is felt far beyond the balance sheet – it is people that are let down, often hard-working volunteers or people in desperate need. That's why I'm urging all trustees to take action now, to protect their charity's valuable funds and assets. Charity brings immense value to society, not just through the good work charities do directly, but also in its power to promote cohesion, well-being, and pride in our society. This is more important than ever, so the fact that there are those who wish to exploit public generosity and charitable endeavour for selfish, criminal purposes is appalling. Combating fraud is vital to giving people confidence that their money is safe and will go to the causes they care so deeply about.'

Read the Action Fraud article here

National Cyber Security Centre provide small businesses revamped cyber guide

Early this month the National Cyber Security Centre published a revamped Small Business Guide for 2020. The publication provides small businesses with information on how to stay safe online and sets out five key areas for businesses to improve their cyber security. The revamped guide is timely, as many organisations have moved their operations online as a result of the coronavirus pandemic. The original guide was published in 2017 and included advice on key areas such as protecting passwords and preventing email phishing attacks. The five key areas recommended in the publication are;

- Backing up your data.
- Protecting from malware.
- Keeping your smartphones (and tablets) safe.
- Using passwords to protect your data.

- Avoid phishing attacks.

Read the NCSC news publication

National Cyber Security Centre provide toolkit to support retailers

In addition to the Small Business Guide, the NCSC has produced a refreshed toolkit with the British Retail Consortium to support trailers boost cyber defences. The toolkit is designed specifically for non-cyber experts such as Board members and those in senior roles. The toolkit outlines recommended actions for retailers in four areas;

- Preventing breaches through stronger protections.
- Preparation to mitigate the impact of a successful breach.
- Recovering after a cyber-attack.
- Developing and embedding a positive cyber resilience culture at Board level.

Read the NCSC press release here

Second lockdown to bring more scams over Christmas

This month The Telegraph has reported that fraudsters will target the elderly and vulnerable should the country enter a second lockdown. Over recent months scammers have taken advantage of the pandemic targeting the public with investment scams. In May this year, Santander reported the worst month for investment scams on records. As fraudsters take advantage of financial uncertainty it is predicted that should a second lockdown be imposed on the UK, scammers may again target the elderly by offering lucrative investments or savings deals.

Read the article here

Fraudsters target government business loans

The BBC has reported this month that fraudsters have targeted the recent COVID-19 business bail out scheme launches to help struggling businesses. The article covers the story of who individual who's personal details were stolen to set up a bogus company and claim £50,000 from the government scheme. The Governments Bounce Back Loan Scheme launched in April. The government has claimed that banks are taking 'appropriate precautions' however, this week The Guardian reported that the head of the National Audit Office confirmed the scheme was most

at risk out of all of the support measures implemented. Although the loans are only to be offered to companies registered prior to 1 March 2020, the BBC report claims that payments have been made to companies registered as late as June. The article also reports a spike in business registrations have risen since the introduction of the scheme.
Read the BBC article here Read The Guardian article 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 November, 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 – 5th November, 10:30 – 12:30, 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 (http://www.friendsagainstscams.org.uk/elearning/surreybucks) or attended one of our live Friends Against Scams sessions, such as the 3rd November course.

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

Other type of fraud examples

Online & Email scams

- Fake Property Listings on Facebook - Scam artists have been using Covid-19 to swindle renters out of their deposits by posting fake property listings on social media and using the pandemic as a reason for not holding viewings. Read more here
- Consumer goods organisation Which? have this week produced an article warning of the dangers of fake Facebook advertisements. The article highlights the importance of doing your research before clicking links and making online purchases from what seem to be legitimate and genuine advertisements. In one case a member of the public contacted Which? to report that they had placed an order with sportswear brand Gymshark by clicking on what they believed to be a genuine social media advertisement. Gymshark confirmed that they only sell items through its official website, any other retailers offering its products are fraudulent. Read the Which? article on fake advertisements here
- HM Courts and Tribunals Service have reported it is aware of a number phishing emails in circulation. The emails claim the recipient has been issued a penalty charge, warning that if payment is not made court action will be taken. HM Courts and Tribunals Services have

stated that it does not issue Penalty Charge Notices. Any the emails look genuine, the public have been advised to look closely at the senders email address. Emails from HM Courts and Tribunals service will be sent from an email with the @justice.gov.uk format. Read the warning here

- It has been warned that another HM Revenue & Customs phishing scam is circulating. The communication claims that recipients are eligible for a government grant. Similar emails have been seen throughout the pandemic claiming to offer financial support from a range of government departments. Typically, these emails require the user to submit personal and financial details on a fake website linked in the communication. HMRC have stated it has detected 130 COVID related financial scams since March, most of which were sent by text message. Read the Which? article here
- Recently Business Cloud magazine has reported on a range of COVID-19 scam emails which are targeting businesses. Many of these emails have been seen throughout the pandemic such as VAT tax relief, TV Licences and Council Tax rebates. Access the Business Cloud article here
- A range of scams relating to Amazon gift cards have been identified. The Guardian have this month reported on a range of these, including social media in which adverts aim to get users to click links to received free of heavily discounted vouchers. In another scam victims email accounts are hacked, with scammers sending emails to the users claiming to be a friend asking them to buy gift cards and send them the codes. Read the full article from The Guardian here
- Over 100 reports have been made regarding an email claiming to offer £1,000 Asda shopping vouchers in return for completing a survey. Typically such methods are used to gain personal or financial information.

Text Scam

- The Chartered Trading Standards Institute (CTSI) has raised a warning over scam texts demanding the public perform jury service or pay to postpone it. The bogus texts invite recipients to perform jury service or delay it at cost. The texts host a link to a scam website clad in UK Government branding which asks the target to confirm that they can perform the service or to postpone jury service for six months at a fee of £34.99. Read here
- Scam text messages have been identified which falsely claim the recipient has been selected for jury service. The communications claim that a payment can be made to postpone the requirement to perform jury service. Official jury summons communications never ask for payment, they will ask recipients whether they can attend the selected dates and to explain any reasons for unavailability.
- Scam text messages from HMRC are doing the rounds. These are from an unknown number and state 'HMRC: Our records show you have an outstanding tax return of £307.72. To claim complete our return form via: https://hmrcpending-rebate.com'
- A sharp increase in scam text messages targeting customers of the Halifax bank has been reported. The message claims that a new payee has been created, with users advised to click the link if they did not request this. The link takes users to a fake site, in an attempt

to steal users log in details. Read the Which? article and guidance here

Other

- Action Fraud has seen an increase in courier frauds, which involves fraudsters impersonating trusted individuals and organisations to trick them into money, bank cards or items of high values, to a courier sent to their home. Recent reports have seen an increase in fraudsters conning victims into purchasing high value items such as gold, scammers send couriers to collect payment for the non-existing products.
- Which? have recently warned that a range of Brexit scams have increase as the UK. Scammers are using the current confusion around Brexit to trick the public in a range of scams, such as into purchasing European Health Insurance Cards (EHIC). The cards give EU citizens the access to state provided healthcare during a temporary stay in another company. The cards are free to obtain from official sources and depending how the UK exits the EU, the card may no longer be required. Scams have also purported to be from HMRC and have targeted UK businesses preparing for arrangements after the transition phase. Phishing emails, along with other communications, have been used citing the need to register for a UK trade number to continue to trade with the EU. These communications aim to steal valuable personal and financial information. Other Brexit related scams include bogus investments and financial services scams. Read the Brexit scam warning by Which? here
- Sky News has reported on recent claims that scammers are pretending to be COVID marshals and medical professionals to trick the vulnerable to gain accesses to their homes. The Chartered Trading Standards Institute have stated that COVID marshals do not have the power to enforce social distancing, issue fines or enter private properties. Read the Sky News article here
- Greater Manchester Police have recently warned the public to be aware of romance scams. Romance related scams have increased during the pandemic, with scammers taking advantage of the isolation caused by lockdowns and local restrictions. Romance scams involve fraudsters slowly gaining the trust of the victim before asking for money, for example to pay for a flight or visa to be able to visit the victim. Click here to access the Action Fraud romance scam article
- A total if £207.8m has been lost to scammers via bank transfer fraud in the first 6 months of 2020. Which? report that although the figure is in line with 2019, most banks have since signed up to additional measures to protect the public from such scams. Read the Which? article here