COVID-19 Fraud & Security Alerts

Ref: CFMG-005

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

NHS Test and Trace emails:

NHS Test and Trace phishing emails are being sent by scammers, the fake email refers to the service as 'track and trace'. The email advises the recipient that they have been exposed to someone who has tested positive for coronavirus. They are instructed to click on a link in order to find out who that person is and are warned that if they fail to do so within 24 hours, legal action may be taken and their benefits suspended. The email address from which this message is being sent is 'alert@nhstrackandtrace233-gov.com'.

Remember, contact tracers will never ask you to:

- Dial a premium rate number to speak to them (for example, those starting 09 or 087).
- Make any form of payment.
- Give any details about your bank account.
- Give your social media identities or login details, or those of your contacts.
- Disclose passwords or pins.
- Create any passwords or pins.
- Purchase a product.
- Download any software to your device.
- Hand over control of your pc, smartphone or tablet.
- Access any website that does not belong to the government or NHS.

Read more here

Crown Prosecution Service (CPS) West Midlands: Successful COVID-19 prosecutions – March to May 2020:

CPS West Midlands Magistrates' Court unit successfully prosecuted 78 COVID-19-related cases over the past three months which included incidents of emergency workers and key workers being assaulted, threatened, coughed at and spat on by people claiming to have COVID-19. Some of the cases against healthcare workers are listed below:

May 2020

- Penelope Russell attended the University Hospital in Stoke on Trent with symptoms of COVID-19. While waiting to be seen she was provided with a mask, but she removed this and deliberately shouted and coughed at a nurse. She denied the offence but was convicted at the trial on 18 May 2020 and received a 26-week custodial sentence for the assault and a further 14-week sentence as she was in breach of a suspended sentence.

March 2020

- Wayne Harvey, from Nuneaton, assaulted a security officer at George Eliot Hospital in Nuneaton who caught him stealing a handbag from the receptionist. He told police he had coronavirus to try to avoid being arrested. He received 31 weeks' imprisonment after pleading guilty at his first hearing at Coventry Magistrates' Court.

Click here to read more

Man arrested for allegedly selling over 500 fake coronavirus testing kits on the dark web

A Birmingham man has been arrested for allegedly selling fake coronavirus testing kits on the dark and open webs, as part of the National Crime Agency's response against criminals trying to exploit the Covid-19 pandemic. He is believed to have sold the kits to customers in the UK and United States.

Read full article here

Fake calls from someone purporting to be from Cifas:

Cifas is a not-for-profit organisation working to reduce and prevent fraud and financial crime. It has been made aware of a fraudster calling fraud victims claiming to be a Cifas employee, offering to get their money back. Be aware that Cifas will never make contact with fraud victims in this way. If you receive this call hang up immediately and never offer up any personal or financial details.

Google launches website to help people avoid online scams (including COVID scams):

Google and Cybercrime Support Network joined forces and launched the website, https://scamspotter.org/. The website tries to show people how to identify things such as bogus stimulus checks, fake vaccine offers, or other false medical information. The site also highlights certain patterns that are typical of hoaxes, like a romance scammer asking you to wire them money or buy them a gift card. The website is especially geared at educating seniors, who disproportionately lose more money than other demographics because of scams, Google said.

Public Sector Counter Fraud Journal

The Government Counter Fraud Profession has published issue 5 of the Public Sector Counter Fraud Journal. The publication provides an update and insight into counter fraud news across the public sector. The publication covers a range of areas, particularly on COVID-19/ Articles include;

- The Government Counter Fraud Function's COVID-19 Response
- COVID-19: Maintaining a controlled environment

- How prepared are insurers for the risk of increasing fraud during and after the COVID-19 pandemic?
- Protecting charities from harm: Fighting fraud and cybercrime
- Coronavirus, fraud risk, and the use of the term “scam”
- Digital detectives in the NHS
- How the UK justice system has adapted to the COVID-19 pandemic
- COVID-19: The risk of fraud in a crisis

Click here to access the publication

Financial Conduct Authority (FCA) Warning List tool

The FCA has a tool to help you check if an investment opportunity is a scam. You can check the type of investment and search FCA’s Warning List of firms that are operating without permission or running scams. You can also check it's an authorised firm on the Financial Services Register and even if it's on the Register, you need to be aware that it might still be a 'clone firm' pretending to be a genuine firm and you should do more checks.

Click here to read more

Download your "Little Book of Big Scams":

The metropolitan Police have issued the 5th edition of the “Little book of big scams”. This book helps raise awareness of some of the ways criminals use to scam the public out of money and to avoid becoming a victim of the Fraudsters. The book covers; fraud enablers; types of fraud; and what to do if you get scammed.

Click here to read the book

ITV Tonight Programme – Scammers

The ITV Tonight programme, a popular current affairs series, last week focused on lockdown scammers. Since February Action Fraud has received over 2,000 reports of COVID-19 related scams, resulting in a loss of over £4.6m. The Programme was originally aired on 28 May and is available on the ITV Hub.

Click here to watch

Business Grants Fraud - Freedom of Information Requests

Cifas has stated that suspected fraud attempts are being reported by local authorities involving a Freedom of Information request asking for business grant payment details. Current policy is to not release a FOI response in relation to this until the scheme is over. The perpetrators are suspected of looking to identify eligible businesses that haven’t applied with a view to put in their own fraudulent application.

National Cyber Security Centre (NCSC) supports US advisory regarding GRU intrusion set Sandworm

The NCSC has warned of a Russian hacker group which has targeted two ministries of foreign affairs and a national parliament using ComRat v4 malware. The NCSC supports the advisory produced by the US National Security Agency regarding GRU (the Russian military intelligence service) intrusion set known as 'Sandworm'. To mitigate the CVE -2019-10149 vulnerability, providers should update Exim immediately by installing version 4.93 or newer.

Read more here

HM Revenue and Customs target furlough fraud

We have previously reported publications addressing the vulnerability of the governments furlough scheme in response to the COVID-19 pandemic. This week the Financial Times report that HMRC have announced plans to target company directors who have flouted the furlough scheme rules. Draft legislation has been published by HMRC which will see plans to recover payments which have been fraudulently claimed. Penalties will also be imposed on companies in cases of fraud.

Read more here

Incident Response (IR)

East Midlands Special Operations Unit has provided guidance on incident response preparation:

1. **Develop policy:** To outline the authority and responsibilities of the IR team. This might include; the revocation of access rights, taking systems offline, reconfiguring them, purchasing equipment and services, accessing sensitive information and conducting forensic investigations. Ultimately, any delays will hinder recovery so outline responsibilities and the means to settle disputes well in advance.
2. **Communication Plan:** Who should the IR team contact in the event of a problem? When is contact appropriate and how should it be made? How will messages be communicated vertically and horizontally across the organisation or to external agencies? How will you be contacted by customers and suppliers? A good communication plan facilitates a realistic appraisal of the ongoing situation and avoids unhelpful speculation during difficult times.
3. **Define critical functions:** Which systems have the highest impact if compromised and how quickly should they be restored? What data would be the most damaging to lose and where is it located? Once you know what the critical functions are, you can prioritise money, time and IR effort protecting them.
4. **Define roles:** To maximise efficiency! Who can lead the IR team, or facilitate purchases? Who will liaise with HR when there's an insider threat or an internal breach of policy? Who has the expertise to deal with applicable laws, regulations and contracts, or the skill and diplomacy to communicate across the organisation and to external entities?
5. **Rate the incident:** To understand the gravity of the situation and elicit the appropriate response across the organisation.
6. **IT hygiene:** Network diagrams, build documentation, recovery procedures, up-to-date inventories and change control documents should

be in order to efficiently sanitise, recover or rebuild infected system and operations.

7. **Ensure network visibility:** Logs must be collated, synthesised and evaluated to identify and track problems across the network. Check - Windows event and security logs, anti-virus and firewall logs, as well as rogue accounts on the network. Alternatively, consider holistic solutions such as SIEM technologies.
8. **Business continuity:** Failing to prepare is preparing to fail. Develop a work around for when there is a complete or partial loss of IT services. How will critical operations continue in the face of such difficulties?
9. **Train:** The identification and resolution of a problem needs an organised response. The IR team need to react to different situations calmly and with confidence which is why it is so important to practice IR by exercising or simulation.

Further advice on incident response, from the NCSC, can be found here.

Other type of fraud examples

Ransomware

- Cifas has reported intel of a banking Trojan effecting the Android operating system which has popped back up. This Trojan is capable of stealing financial credentials, SMS and contact lists. Organisations using Android applications should remain vigilant for this threat. As is the case with most Android banking Trojans, it masquerades as popular applications to infect mobile devices and are, therefore, more likely to dupe potential victims. Research all applications before download, and only download from official app stores.

Email scams & Phishing scams

- Bereavement vishing scams are doing the rounds, where Fraudsters are attempting to con money out of families organising funerals for loved ones. Callers are contacting families claiming to be from the local authority's bereavement services team. They then ask the families to provide card details over the phone in order to supposedly pay the funeral director. They apply pressure to the suffering families by telling them that the funeral will be cancelled if they don't pay. The council has put out an urgent warning on its social media channels, warning about the threat. Individuals receiving such calls are encouraged to report incidents to Action Fraud.
- We have previously reported TV Licensing phishing scams have been reported during the pandemic. These emails continue to circulate, typically asking users to update direct debit details, or offering a COVID-19 six month free TV Licence offer. Action Fraud has received 260 reports of this scam in May alone. Read more here.
- Likewise, HMRC phishing emails continue to circulate. A Financial Times investigation this week reported that the number of emails reported to HMRC had increased to 42,575 in March, an increase of 74% since January. Read the full article here.
- Early reports are circulating of emails purporting to be from Deutsche Bank offering one year interest free loans. The emails offer the loans of between £5,000 and £100,000 without credit checks with a 2 day approval. The contact details provided are for an outlook

email address.

Phone Scams

- Amazon Prime renewal scams have been circulating again. An automated scam call is impersonating Amazon Prime, telling victims their subscription will be 'renewed' for £39.99. The scam phone call is designed to trick Amazon Prime customers into connecting with a fraudulent 'account manager' and from here, it's highly likely scammers will attempt to extort bank details and/or personal data from you. https://conversation.which.co.uk/money/amazon-prime-renewal-scam-phone-call/
- West Yorkshire Trading Standards has been receiving reports about a rogue trading company that has been cold-calling people. The 'business' claims they are concerned with the air in your area and send a letter stating that they need to 'come and check if the air is fresh' - and if not will clean it to 'prevent the coronavirus'. Residents are also being advised to look out for fake PPE (Personal Protective Equipment) that is being offered across West Yorkshire.

Online Retailers / Counterfeit goods

- Cybercriminals have been busy establishing dozens of fake websites that impersonate the domains of popular UK supermarket chains. Thirty lookalike domains impersonating Tesco, 11 illegitimate domains impersonating Asda, and 10 recent spoofed websites impersonating Amazon have been uncovered. These fake domains can enable hackers to obtain names, addresses, email addresses, and payment card information of hundreds of thousands of shoppers in a very short time.

Social media and other messaging platforms

- Adverts and Facebook pages have started popping up for 'freshers' welcome parties and events planned for September 2020 with young people being targeted to buy tickets for non-existent events. These scams are preying on freshman's hopes that their fresher week will be a normal experience post lockdown – but what 2020's fresher week will look like is still up in the air. To confirm legitimacy contact your Student Union to verify any student events before you hand over your hard-earned cash.
- Phishing messages are circulating on WhatsApp purporting to be from chocolate confectionary company Cadburys. The messages suggest that company is giving away chocolate hampers. They require users to provide personal details and also share the message to other contacts.
- Text messages purporting to be from the UK Government inform recipients their movements have been tracked through phones and they have breached lockdown rules. The messages state a fine must be paid, in order to prevent a more severe penalty. Trading Standards have warned to ignore these messages and not to click any links. The sender may appear on phones as "UK_gov".

Text Scams

- Scam texts appearing to be from Barclays have been identified informing recipients that a fictional new payee 'R Davies' had been added to their account. The recipients are then invited to click a link if this additional payee was not authorised. This would then led potential victims to a website that has used images and wording copied from the real Barclays website, asking for login details including their membership number, card details, and proof of identity.