COVID-19 Fraud & Security Alerts

Ref: CFMG-006

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

Man offers discount to NHS workers on fake car insurance

A man was arrested yesterday by the City of London Police for acting as a 'ghost broker', selling fraudulent car insurance, and recently offering the same to NHS workers at a discount.

Click here for more details

Update: Fraud threats to the NHS from Covid-19

The impact of Covid-19 on fraud within the NHS was highlighted in the NHS Counter Fraud Authority's (CFA) Intelligence Report: Fraud threats to the NHS from Covid-19 April 2020. However, the landscape of fraud changes so rapidly that assessment updates have been published which highlights further merging threats, vulnerabilities and enablers of fraud. The updates provided includes: a list of threats covered in the Intelligence Report; additional emerging threats; and NHSCFA reporting figures.

A list of all the threats included in the Intelligence report and updates are: cyber enabled fraud; false information; death certificates; agency fraud; staff fraud; procurement and commissioning fraud; pharmaceutical contractor fraud; payment by results (PbR) fraud; general practice (GP); contractor fraud; help with health costs fraud; NHS volunteers; procurement and commissioning markers; fraudulent access to the NHS without charge; European Health Insurance Card (EHIC) fraud; NHS bursary fraud; dental contractor fraud; optical contractor fraud; NHS charities; fraudulent appeals; personal health budgets; handling stolen goods; additional fraud threats and warnings; contact tracing app-Bluetooth; contact tracing app-Phishing SMS; cyber enabled fraud-business loans/grants; cyber enabled fraud-data harvesting; NHS continuing health care (CHC) plans-Assessments; NHS staff-private work; SARs & money laundering; dental practices disregarding COVID-19 SOP; and impersonation of NHS Staff to avoid lockdown restrictions.

These publications and updates are available on the NHSCFA Extranet which is currently available to Local Counter Fraud Specialists and Directors of Finance.

Major VMware server vulnerability detected

A major VMware code injection vulnerability that left private clouds exposed to malicious actors has been discovered.
See NCSC weekly threat report for the link to the advisory published by VMware to patch this flaw.

Remote workers targeted by Office 365 phishing scam

Cyber criminals have been targeting remote workers with a phishing attack that seeks to steal user credentials. The scam sees attackers send staff an email pretending to be from their organisation's IT department. It requests users update the VPN configuration used to access the company network while working from home. Users who click the link in the email are directed to a fake page that looks identical to a legitimate Office 365 login page. Staff who are misled into entering their credentials give the fraudsters the details to their Office 365 account.
Cyber criminals constantly look for new opportunities to trick people into revealing sensitive information. NSCS has provided advice on spotting and dealing with phishing emails and messages here.
The NCSC has published a range of guidance to support organisations with remote working here.

Multiple Vulnerabilities identified by Cisco in their Adaptive Security Appliance (ASA) Software and Firepower Threat Defence (FTD) software and routers

The National Cyber Security Centre (NCSC) has reported that multiple vulnerabilities have been identified by Cisco in their ASA and FTD software and routers which could allow an unauthenticated, remote attacker or an authenticated, local attacker; to conduct directory traversal attacks and obtain read and delete access to sensitive files on a targeted system; to execute arbitrary code on an affected system or cause an affected system to crash and reload.
See NCSC weekly threat report for links to advisories provided by Cisco.
In both advisories, Cisco have included the latest software releases that will address these vulnerabilities for software and routers and at present there are no workarounds available.
The NCSC recommends following vendor best practice advice in the mitigation of vulnerabilities. In this case, the most important aspect is to install the latest software version. Guidance has been published by NCSC about keeping all devices and software up to date.

Furlough fraud: 1 in 3 pressured into working

Furlough fraud has suffered a rise in recent weeks, with the government now receiving close to 1,900 reports of fraudulent use of the Job Retention Scheme established by the Treasury. The research, which surveyed 2,000 workers in the UK, showed people were being pressured in numerous ways. 27% said they were asked to send and respond to emails, with 17% asked to make phone calls. The research also showed 12% are being pressured to attend their workplace physically, and 11% to work for the company as a "volunteer".
Read here for more

Latest fraud figures show the scale of Covid-19 scam attacks – as TSB reveals cases and vital support for victims

Latest figures show that the number of scam cases reported to Action Fraud exceeding 2,100 since February, with losses passing the £5million mark this week. The data also shows that over 11,500 reports of coronavirus themed phishing scams have been lodged as fraudsters impersonate a variety of organisations relevant to the handling of the virus and lockdown measures.

Recent TSB research shows that 42% of Brits suspect they have been targeted and that one in 10 people know someone who has been defrauded over the lockdown period. Throughout the pandemic, TSB has shared details of emerging scams with the public and provided expert industry insight to help people avoid fraudsters' new tricks. TSB and Cifas have also identified the most common Covid-19 scams Brits have been targeted with during the pandemic.

Read here for more

Storage pod owners attempting to cash in on grant scheme:

Intelligence received by Cifas this week reported over 580 storage pods have applied for business rates relief grants. This is due to the storage pods being classed as individual properties (according to tribunal decisions). These pods are not businesses and are investments linked to personal pension plans and therefore fall outside of the grant scheme - Storage pod owners attempting to profit off of the scheme.

Kill Chain

East Midlands Special Operations Unit (EMSOU) has provided advice on kill chain as follows:

The term kill chain describes how an organisation's network might be attacked.

Reconnaissance: Assess the organisation from the outside-in, to identify targets and tactics. Tactics used may include scanning networks for known vulnerabilities and using open source intelligence (corporate websites, news reports and social media profiles).

Intrusion & Exploitation: Attackers can exploit identified vulnerabilities to penetrate the network and/or use what has been discovered to socially engineer an attack - manipulating staff to; click a link, download malware, visit an infected website, or plug in a malicious USB.

Expansion & Entrenchment: Once access had been gained, the attackers move laterally to other systems and accounts (privilege escalation), to obtain access to high value data or better control of the network. Purpose built penetration tools are 'noisy' so many attackers will 'live off the land' and use inbuilt functions, such as PowerShell, and tap into file systems (NFS and SMB) which pass information over the network unencrypted.

Exfiltration & Damage: Attackers will; steal data piecemeal or en masse, deploy a payload such as ransomware or a logic bomb, biding their time for maximum effect.

Covering your tracks: Attackers will purge log files, delete temporary files and software, plant 'false flags' and encrypt drives to confuse and delay any form of forensic investigation.

Why it matters?

The Kill Chain emphasises the need for defence in depth employing a multi layered approach involving technical, procedural and physical

controls:

- Logical controls (vulnerability scanning; host hardening, segmentation, anti-malware)
- Administrative controls (policies; procedures, standards, training)
- Physical controls (gates, doors, badges, signage, equipment disposal etc.)

The kill chain illustrates how large the attack surface is for an organisation and the time and commitment a cybercriminal will invest in attacking your organisation.

The average amount of time an adversary will spend in the network before launching an attack - known as the dwell time - is 6 months.

When preventative controls fail, an organisation's survival will depend on:

- Detective controls: to identify, flag and trace intrusions.
- Recovery controls: to contain, sanitize, restore or recover the network.

Table top sessions are a key element in the defence of any organisation against a cyber event.

Gathering critical team members, to discuss ways to; identify, study and respond to different types of cyber incidents and maintain business operations will ensure survival. "Failing to prepare means preparing to fail."

SARS in Action, Issue 5 May 2020

The Nation Crime Agency (NCA) has published a special edition of their 'Suspicious Activity Reports' (SARs) in Action magazine. There were an estimated 3.8m incidents of fraud in the year ending September 2019, and this issue shines the spotlight on this crime which has such a profound economic and human cost. The magazine includes articles on the 'SARs analysis on COVID-19', ' New drive to tackle COVID-19 crime' and 'SARs value in fighting NHS fraud'.

Click here to read full article

Webinars

- The role of technology in detecting and preventing financial crime post COVID-19, on Wednesday 17 June 2020 at 11am (Duration: 1 hour)
  This webinar takes a deep dive into the consequences of COVID-19 to the financial services industry, and how using technology can future-proof your business to keep moving forward.
  Read here for more details and to register
- Preventing cybercrime for charities: getting the basics right (Live interactive online session), on Wednesday 17 June 2020 at 12:30 - 13:30 and Friday 19 June 2020 at 12:30 - 13:30
  This two-part briefing, delivered by the City of London Police's Cyber Griffin team, will outline the ways you can defend yourself against the most common attacks. It is non-technical so suitable for everyone, everywhere! Each session will be live and followed by a Q&A.
  Read here for more details and to register

Other type of fraud examples

Ransomware

- Criminals are using malicious CV and medical leave forms to spread banking Trojans and information stealers. When opening the attached file, victims are asked to "enable content" and when they do, a malicious macro starts running, downloading the malware. Once a device was infected, threat actors could use the malware to carry out financial transactions on the device.
- EMSOU has warned that there is expected to be a spike in ransomware attacks as employees return to their physical workspaces. Due to the short amount of time to prepare employees for remote working, security protocols and procedures were relaxed in some organisations. Ransomware on potentially compromised devices are expected to be activated when returned to the workspace.

Email scams & Phishing scams

- The Health and Safety Executive (HSE) is aware of malicious emails reportedly coming from a HSE address. Please note these are not officially sent from HSE. HSE advises anyone who receives a message not to click/open any documents and delete the emails. There is no need to contact HSE.
- A new Amazon phishing campaign has emerged claiming to offer recipients the chance to win a £1,000 Amazon gift card. The subject reads: "On the occasion of overcoming the coronavirus, Amazon gives you the gift of victory." The sender name is spoofed to read contact@amazon.com. The recipient is instructed to click on a link in order to apply. The link has been identified as malware.
- Fake voicemail notifications are targeting remote workers. Attackers have devised a new phishing campaign that distributes emails that look as if they were generated by PBX, a legacy technology that integrates with employees' email clients so they can receive their voicemail recordings. Researchers found this has threatened nearly 100,000 mailboxes around the world, across multiple sectors. PBX is a useful tool for employees who lack convenient access to their office landlines, increasing usage due to COVID-19. Actors are now crafting email subject lines designed to trick recipients into thinking they have received a new voice message. Malicious attachments drive recipients to a fake landing page for credential harvesting e.g. their O365 login credentials. Actors use highly targeted subject lines that include a specific company's or person's name. The emails do not bear an actual malicious payload and can bypass secure email gateways.
- A 'DHL Overdue Account Notice' email is doing the rounds and the sender name reads 'DHL Accounts Receivable Dept. [mailto:noreply@dhl.com]' and asks you to click on a link for more details. Do not click on any links and contact DHL directly for any queries.

Phone and Text Scams

- Police continue to warn people to be wary if scammers calling and pretending to be part of the NHS Test and Trace service. See last

week's alert for details on how to look out for these scammers. Remember if you are contacted by the NHS Test and Trace service, you will not be asked to provide any passwords, bank account details or PINs.

- Action Fraud are aware of scammers claiming to be from HM Revenue and Customs (HRMC) offering financial support as a result of coronavirus. If you receive a text, email or call claiming to be from HMRC that asks you to click on a link or give info such as your name, credit card or bank details, it's a scam.
- Fake lockdown fines, which involved victims being contacted by bogus text messages claiming to be from the government.
- EMSOU have reported that scam texts purporting to be from Sky, GOVUK and HMRC are being seen and reported locally. Examples include the following: "I received notification of the Sky engineers visit earlier in the week scheduled for 1 June and a text message from the Sky messaging service on Sunday as a reminder and the engineer called yesterday. I have changed my sky password, blocked this number and deleted the message."; "Just had a call from 01227 126302, a recorded message from HMRC stating there was a tax fraud against my name. I didn't get to the end of the message deleted and blocked the number."; "GOVUK: You may be eligible for a COVID-19 relief fund of up to Â£1,500.00 please complete the application form with the link below to check your eligibility."; Hi ___ it's Sky. We'd like to come and attempt your Sky visit soon. Your engineer will attempt to complete the work from outside your property, but to get your services fully up and running, they may need to come into your home. We have clear guidance to keep you and your engineer safe. If you'd like to go ahead, we have an engineer available on 29/05/2020. If you'd like to reschedule your visit to this date, please reply YES. Please reply within 24 hours."

<u>Online Retailers / Counterfeit goods / Door to Door</u>

- Fraudsters are posing as nurses on dating sites. The National Crime Agency director general stated, "We've seen reports of a dating fraud where people are pretending to be a nurse in a hospital stating that they 'need money to help get to work'. Never send money or offer financial details to strangers online. Click here to read more
- Confused.com received an alert from a member of the public about a door to door salesperson visiting their home (HP2 postcode) purporting to be from Confused.com. The individual was attempting to sell insurance products and was requesting personal details from the homeowner. This is fraudulent as Confused.com is an entirely online service. If this occurs to you report it to your local police force by calling 101.

<u>Social media and other messaging platforms</u>

- HRMC have warned students to beware of scams relating to a fresh wave of cyber frauds offering bogus tax refunds. Check online for information on how to avoid and report scams here.
- Action Fraud has received over 300 reports since January 2020 about Snapchat accounts being compromised as a result of users being

tricked into handing over their log-in or two-factor authentication (2FA) codes. In some cases these victims are being extorted for money with the threat of having their private photos being shared publicly.

Spoof websites / emails

- CIFAS warn of a new HMRC scam, specifically targeting people who are out of work or working less due to coronavirus. The scam claims to offer thousands in grants and recipients are told to click a link to check eligibility. The questions asked on this link are designed to steal personal information. The email address used in this scam is: HMRC@hotmail.com.
- Legitimate companies are being impersonated and are offering fake jobs to members of the public. This threat is largely focused on fraudsters harvesting data from victims under the guise of accepting a job role. Once the fraudsters have gathered the personal data, they impersonate the victim, taking over their motor insurance policy and submitting false claims.