Counter Fraud Services

Protecting Resources
Delivering Solutions

Rolling COVID-19 Intelligence Alert 11 May 2020

OFFICIAL-UNMARKED

Fraud.
Together we can stamp it out.

Introduction

The Rolling COVID-19 Intelligence Alert has been compiled from a number of partners websites to provide a one-stop shop reference guide about scams and frauds to protect NHS Scotland and its members of staff and their families from fraud during COVID-19.

How to Use the Document

The document is split into two tables. The first provides intelligence on “Protecting NHS Scotland from fraud during COVID-19”, and the second concentrates on “Protecting NHS Scotland members of staff and their families from fraud during COVID-19”. To find the information you are looking for use the search facility in Adobe. This should help you to find any information on the topic you are looking for, if available. A brief summary of advice and guidance on the topic is provided along with the associated link to allow you to find out more detailed information.

Counter Fraud Advice

Detailed counter fraud advice is available online including from

- Scottish Government Cyber Resilience Unit;
- National Cyber Security Centre;
- Police Scotland;
- Trading Standards Scotland;
- Scottish Business Resilience Centre;
- Advice Direct Scotland;
- Get Safe Online; and
- Action Fraud.

Scottish Government Cyber Resilience Unit

As a result of the significant rise in COVID-19 related scams, the Scottish Government Cyber Resilience Unit is sharing important information from trusted sources via a regular 'Cyber Resilience Notice' for business organisations, public sector organisations, charities and the general public. Brief details of the latest scams and advice are provided in this document with the relevant link to the Cyber Resilience Notices.

National Cyber Security Centre

The National Cyber Security Centre (NCSC) is the UK authority on cyber security and supports the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public. The NCSC, a part of GCHQ, has launched the cross-governmental 'Cyber Aware' campaign, which offers actionable advice for people to protect passwords, accounts and devices. The campaign encourages people to '*Stay home. Stay Connected. Stay Cyber Aware*', and its top tips for staying secure online are:

- Turn on two-factor authentication for important accounts
- Protect important accounts using a password of three random words
- Create a separate password that you only use for your main email account
- Update the software and apps on your devices regularly (ideally set to 'automatically update')
- Save your passwords in your browser
- To protect yourself from being held to ransom, back up important data

Police Scotland

Police Scotland is working with a number of partners on the Shut Out Scammers campaign. The campaign signposts the public to relevant prevention advice and support services. These include: Trading Standards Scotland; Scottish Business Resilience Centre; Advice Direct Scotland and the Metropolitan Police.

Top tips to prevent procurement fraud: Police Scotland offer top tips to prevent procurement fraud:
1. Ensure all staff who are able to make or are involved in financial decisions are trained how to identify procurement fraud.
2. Never give in to pressure or threats that it is a time-sensitive issue or an urgent matter. A genuine organisation will have no issues with you verifying a request, however a fraudster will often try to pressurise you into acting immediately.
3. Ensure a three-way match is carried out. Do the amounts documented on the requisition, purchase order and invoice all align?
4. Adopt dual control procedures for authorising payments. Ensure that a senior member of your team reviews your actions and formally authorises the payment.
5. Ensure the procurement process is followed and is enforced. Has an order been placed before the procurement paperwork has been raised? If so, why?
6. Carefully check the sender's email address to identify if it exactly matches your known and trusted records and call your supplier to verify the email is genuine
7. Be vigilant to any clerical or spelling errors within emails which may indicate the email is fraudulent.
8. If it is a new supplier, carry out internet searches to check if they are genuine, are there any customer reviews and phone any listed landline to check.
9. Be alert to any requests to alter bank details. Carry out an internet search of the new bank account sort code and account details to uncover: Location of the bank (to be checked against the company address) and whether there are any blogs or reports available to indicate the communication is a scam.

Trading Standards Scotland

Trading Standards Scotland (TSS) issue a weekly ebulletin **Scam Share** in which they list some of the most recent scams reported by consumers across Scotland. Phone, email and online scams are constantly evolving, and they want to make sure that consumers are aware of as many of them as possible. Brief details of the latest scams and advice are provided in this document with the relevant links to the Scam Share ebulletins.

Scottish Business Resilience Centre

The Scottish Business Resilience Centre (SBRC) is a non-profit organisation which exists to support and help protect Scottish businesses.

The SBRC unique connection to Police Scotland, Scottish Fire and Rescue Service and Scottish Government gives SBRC exclusive access to the latest information on legislation, criminal trends and threats, allowing SBRC to provide the very best advice to safeguard Scottish businesses including their staff and customers.

SBRC offer a wide range of business resilience services, delivered by their expert team of trusted professionals, seconded police and fire officers and innovative Ethical Hacking students from Abertay University. SBRC work in partnership to protect people, places and processes and are constantly looking at new ways to keep businesses free from risk.

Advice Direct Scotland

For advice on your consumer rights during the COVID-19 outbreak contact Advice Direct Scotland on 0808 164 6000.

Metropolitan Police

The Little Book of Big Scams published by the Metropolitan Police provides details of the most common fraud techniques.

Get Safe Online

Get Safe Online is the UK's leading source of unbiased, factual and easy-to-understand information on online safety. The website is a unique resource providing practical advice on how to protect yourself, your computers and mobiles device and your business against fraud, identity theft, viruses and many other problems encountered online.

In addition to COVID-19 specific content the site contains guidance on many other related subjects too – including performing backups and how to avoid theft or loss of your computer, smartphone or tablet. Every conceivable topic is included on the site - including safe online shopping, gaming and dating.

Reporting

NHS Scotland Fraud

There are three options to report NHS Scotland fraud:

Online 

or

Call the Fraud Hotline on 08000 15 16 28 

or

Write to us at: Counter Fraud Services, 3 Bain Square, Livingston, West Lothian, EH54 7DQ.

The online reporting form and hotline are hosted by and powered by

CRIMESTOPPERS

All information provided will be treated in strictest confidence.

Police Scotland and Advice Direct Scotland

Trading Standards Scotland play an important role in both raising awareness and enforcement. As such seek support in reporting any suspicious activity including cold callers or doorstep scammers, and encourage the reporting to **Police Scotland on 101**, or for concerns about a purchase that you have made contact Advice Direct Scotland on 0808 164 6000.

Take Five To Stop Fraud

Stop - Taking a moment to stop and think before parting with your money or information could keep you safe.

Challenge – Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

Protect – Contact your bank immediately if you think you've fallen for a scam.

Report a crime or incident to Police Scotland by calling 101. https://takefive-stopfraud.org.uk/

Action Fraud

Action Fraud is the reporting centre for fraud and cybercrime in England, Wales and Northern Ireland **but not Scotland (where Police Scotland should be notified instead on 101)**. Whilst Action Fraud do not cover Scotland they are well placed to report and advise on fraudulent scams of all descriptions. The Action Fraud main webpage is a source of news reporting on COVID-19 related frauds and you can follow them on Twitter to get update information on COVID-19.

Table 1: Protecting NHS Scotland from fraud during COVID-19			
Date	**Topic**	**Links to sources**	**Advice and Guidance**
07 May 20	**Scottish Government Cyber Resilience Unit** - healthcare bodies at risk of malicious cyber activity	Cyber Resilience Notice - 7 May 2020	**The National Cyber Security Centre (NCSC) and Cybersecurity & Infrastructure Security Agency (CISA) continue to see indications that Advanced Persistent Threat (APT) groups are exploiting the COVID-19 pandemic as part of their cyber operations and have issued a second joint advisory. The joint NCSC/CISA advisory from 8 April 2020 detailed the exploitation of the COVID-19 pandemic by cyber criminals and APT groups. This joint NCSC-CISA advisory provides an update to ongoing malicious cyber activity relating to both national and international COVID-19 responses. Organisations at risk include healthcare bodies, pharmaceutical companies, academia, medical research organisations, and local government. The document describes some of the methods criminals are using to target organisations and provides mitigation advice.** **For more information and what to do to reduce the risk view Cyber Resilience Notice - 7 May 2020**
07 May 20	**Trading Standards Scotland** latest scams across Scotland.	Scam Share - Bulletin 8	**ScamShare Signposts - Each week TSS will signpost key messages relating to different types of scam which are prevalent across Scotland. This week, TSS have highlighted five points relating to business fraud:** 1. **Question** unexpected emails which request private business information or payments, even if they appear to come from someone within your company. 2. **Think** about what you are being asked to do – if in doubt about financial transactions or changes to Direct Debits get a second opinion from a colleague or manager. 3. **Be cautious** when working from home if you receive cold calls offering tech support for your IT system. Only deal with your official IT support desk, if you have one

Table 1: Protecting NHS Scotland from fraud during COVID-19			
Date	**Topic**	**Links to sources**	**Advice and Guidance**
			4. **Confirm** requests for payment or sensitive information with the person or company who has supposedly sent them, using contact information that you know to be correct 5. **Remember** that scam emails and texts can look genuine and can appear to come from Government agencies, people within your organisation and trusted companies. **For more information and What to Do view Scam Share - Bulletin 8**
06 May 20	**Bank Mandate (Account Takeover) Fraud**	Government Counter Fraud Function - COVID-19 Fraud Response Team Cyber Resilience Notice - 7 May 2020	**The threat from mandate fraud has increased during the COVID-19 response. This could result in organisations losing substantial amounts of money that will be difficult to recover.** The threat from mandate fraud is increasing because the public sector has had to rapidly adapt to new ways of working and is necessarily spending money quickly to deal with COVID-19. This has created new vulnerabilities, which criminals are seeking to take advantage of. This type of fraud carries low risk and potentially high rewards for criminals. The Government Counter Fraud Function have already seen instances of attempted mandate fraud around the COVID-19 response. We should not underestimate the sophistication of this fraud. It is not just people emailing to ask for bank accounts to be changed, those attempting it have often harvested information on their targets and use sophisticated techniques to impersonate your suppliers. **Police Scotland have published an article on what you need to know about mandate fraud as well as on their keep safe pages.**

Table 1: Protecting NHS Scotland from fraud during COVID-19			
Date	**Topic**	**Links to sources**	**Advice and Guidance**
30 Apr 20	**Trading Standards Scotland** latest scams across Scotland.	Scam Share - Bulletin 7	This Bulletin highlights a number of issues including: • **Supplier Mandate (Account Takeover) Fraud -** Businesses, charities and individuals should be wary of fraudulent emails which appear to be from trusted suppliers or companies advising that their bank account details have changed. The recipient is asked to make future payments to a new bank account, which is often run by fraudsters. The UK Government has issued advice for charities to help them avoid cybercrimes and mandate fraud. **For more information and What to Do view Scam Share - Bulletin 7**
16 Apr 20	**Scottish Government Cyber Resilience Unit** - PPE and Procurement Scams	Cyber Resilience Notice - 16 April 2020	The FBI and Euorpol have issued warnings after becoming aware of multiple scams involving PPE which is in short supply globally. One example involved a man defrauding a French pharmaceutical company out of €6.64 million by pretending to be a legitimate company and advertising fast delivery of FFP2 surgical masks and hand sanitisers. **For more information and what to do to reduce the risk view Cyber Resilience Notice - 16 April 2020**

Table 1: Protecting NHS Scotland from fraud during COVID-19			
Date	**Topic**	**Links to sources**	**Advice and Guidance**
01 Apr 20	**Tax Avoidance** Advice to help workers returning to the NHS	CFS Intelligence Alert: 01 2020/21 HMRC	**HMRC is aware that unscrupulous promoters of tax avoidance schemes are targeting workers returning to the NHS to help respond to the COVID-19 outbreak.** If you are returning to work for the NHS, HMRC is warning you to be very careful not to sign up to these schemes, which HMRC considers to be tax avoidance.
23 Mar 20	**Bank Mandate (Account Takeover) Fraud** Advice to help members of staff to protect NHS Scotland against increased risk of bank mandate fraud.	CFS Intelligence Alert: 11 2019/20 Police Scotland	**Members of staff should extra vigilant, particularly around Bank Mandate (Account Takeover) Fraud** • Scrutinise requests for: ➢ Urgent payment due to cash flow problems ➢ Changes to bank account details ➢ Contact from third parties requesting changes to bank details and claiming to act on behalf employees incapacitated by COVID-19 **For a full list of DO'S and DON'TS visit Police Scotland**

Table 1: Protecting NHS Scotland from fraud during COVID-19			
Date	**Topic**	**Links to sources**	**Advice and Guidance**
18 Mar 20	**Cybercriminals - Phishing attacks** Advice to help NHS members of staff protect themselves at work against increased phishing attacks.	CFS Intelligence Alert: 10 2019/20 CFS - YouTube video NCSC - Phishing attacks: dealing with suspicious emails and messages	**Email containing malicious attachments and links** • Before opening any attachments or clicking links consider the following: ➢ Is the email unexpected? ➢ Is the email rushing you to do something? (e.g. login in now to reset your password) ➢ Is the email asking you to change security settings? (e.g. enable macros in Word) ➢ Is the email from someone you don't know/trust? **Websites containing fake or misleading information and malware** • Before opening websites consider the following: ➢ Is the website a reliable source? (e.g. Government, NHS, Professional body) ➢ If it asks you to install any software…DON'T ➢ If it claims your device is infected with a virus…close the site and contact your local IT Service Desk **Fake/Malicious apps disguised as COVID-19 information services and trackers** ➢ Only install apps from trusted app stores (e.g. Amazon Appstore, Apple Store and Google Play) NOTE: Malicious apps do sometimes get into these app stores ➢ Do you really need to install the app? ➢ Keep your mobile phone up to date.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
07 May 20	**Trading Standards Scotland** latest scams across Scotland.	Scam Share - Bulletin 8	This Bulletin highlights: • **Travel Cancellations -** Update on Bulletin 7. • **Cancellation Rights -** Due to the number of complaints received about weddings, private events, holiday accommodation, nurseries and childcare, the Competition and Markets Authority (CMA) has established a COVID-19 taskforce to investigating businesses who are not respecting cancellation rights. Issues raised by consumers include being pressured to accept vouchers instead of a cash refund, which may not be financially protected, venues refusing to provide any refund or companies asking people to make a claim on their insurance in order to recover their money.. • **Doorstep Scams -** Communities in Fife have been urged to be wary of cold callers who have been visiting households, claiming to be council workers and offering to disinfect their doorbells. Despite the lockdown, doorstep scammers are still active in communities across Scotland. In addition to scams related to COVID-19 such as offering to disinfect driveways or posing as charity workers and NHS staff, more traditional doorstep scams are continuing. • **Zoom Scam** - The Scottish Business Resilience Centre (SBRC) this week flagged up new phishing emails linked to Zoom, the popular web conferencing tool. These emails were uncovered by threat researchers at Sophos Labs. Scammers are sending emails which appear to be from work colleagues, inviting you to an important meeting or conference. The invitation link takes you to a clone of the real Zoom website, where you will be asked for your email password. If you are invited to join a Zoom call, you should not need to enter your password. Find guidance and factsheets to help you use Zoom and other video conferencing

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			software safely on the **SRBC website**. • **Fake Medical Products -** The Medicines & Healthcare Products Regulatory Authority (MHRA) have launched a new website to allow the public to report any suspected side effects from medicines or medical products relating to COVID-19 treatment. They have also investigated an increasing number of bogus medical products being sold through unauthorised websites claiming to treat or prevent COVID-19. At this time, there are currently no medicines licensed specifically for the treatment or prevention of COVID-19. Any products or cures advertised may be fake and potentially dangerous. • **Phone Scams: Solar Panels -** There have been recent reports from Scottish Consumers of nuisance calls from companies offering solar panel servicing. Customers who already have solar panels are being mis-sold warranties, repairs or upgrades for solar inverters. They are wrongly told that they need to replace or upgrade their inverters by salespeople who take advantage of a lack of understanding about what inverters actually do. • **PayPal Scam -** Scottish consumers have recently received scam text messages and emails which appears to be from PayPal. The following text was reported to Neighbourhood Watch Scotland through their Alert system: "Your account has been restricted due to a failed payment. Please login at ...to remove any pending restrictions." By clicking on the link provided in the email, you could be taken to a legitimate-looking website with PayPal branding, which will ask you to enter personal details and your password. • **Counterfeit Goods online** - Vistalworks have warned that, as people have been turning to home fitness during lockdown, there could be an increase in the sales of

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			counterfeit sportswear online. They have also published a blog about the dangers of using counterfeit hair dyes, at a time when several popular shades are sold out in supermarkets due to increased demand. Use the Vistalworks checker to check the legitimacy of products on Ebay before you buy them. It is also available as a Chrome browser plugin, which will trigger a warning on any suspicious Ebay products or sellers. • **Sextortion Scams -** Police Scotland are warning about recent 'sextortion' scam emails which have been sent to people across Scotland. The email recipient is told that the sender has footage of them watching adult content online and that this footage will be published unless they send the fraudsters a payment in Bitcoin. One Scottish consumer recently reported an email to which threatened to send an incriminating video of them to everyone on their mailing list unless they sent a Bitcoin payment. According to the recipient, the sender used a 'normal-sounding' name to try to make the email seem genuine. • **Illegal Money Lending -** Loans from illegal money lenders end up costing on average three times as much as a legal loan, with some charging interest rates of as much as 120,000%. If you are in a financially desperate situation because of #COVID19, or if you work with vulnerable people and suspect that they may have borrowed money from a loan shark, the Scottish Illegal Money Lending Unit can provide advice and support. Their free and confidential 24-hour hotline will remain open 7 days a week throughout the lockdown period - call **0800 074 0878** or fill out their online reporting form. **For more information and What to Do view Scam Share - Bulletin 8**

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
07 May 20	**Scottish Government Cyber Resilience Unit -** Sharing important information and guidance on COVID-19 related scams.	Cyber Resilience Notice - 7 May 2020	**Trending Topics:** • **Communicating online during COVID-19** - We all remain separated from loved ones due to physical distancing, and many of us are keeping in contact with each other through online communication; for example, through video chats. We have heard of people lending devices to older relatives, or dropping them in to care homes, for example, to enable this contact. Please remember that devices should be secured with a password (ideally three random words), and that care should be taken when joining WiFi. WiFi in public settings should be password protected as well. The NCSC offer a wealth of advice and guidance relating to such matters as the use of passwords and the use of devices such as mobile phones and tablets; and specific guidance relating to common questions (for example, relating to the use of WiFi). • **NHS Covid symptom tracker app – NCSC security -** Experts from the National Cyber Security Centre have been supporting the development of the NHS COVID-19 contact tracing app, which will be launched on the Isle of Wight this week. The privacy and security of app users' data is a priority and the NCSC has been advising on best practice throughout the app's development. They have published three documents relating to the work, including a technical paper which provides a high-level overview of the security and privacy characteristics of the app. You can read more their website. • **NCSC Suspicious Email Reporting Service** - As part of the Cyber Aware campaign, the NCSC successfully launched its suspicious email reporting service (SERS), resulting in dozens of malicious web campaigns being shut down in its first day, after a spike in coronavirus phishing scams. In just over two weeks since

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			the NCSC and police launched the service, the public have passed on more than 160,000 suspect emails, with more than 300 bogus sites taken down. By forwarding any dubious emails – including those claiming to offer support related to coronavirus – to report@phishing.gov.uk, the NCSC's automated programme will immediately test the validity of the site. Any sites found to be phishing scams will be removed immediately. • **Anti-Virus -** An anti-virus firewall software provider (Sophos) recently revealed that cyber criminals exploited an SQL injection vulnerability in their management interface to extract user data such as usernames, passwords, and local device administration information. Sophos have released a "hot fix" for devices that have auto-update turned on. All customers should take note of the further advice on remediation, whether they have received the hot fix or not. You can read NCSC statement following this discovery on their website. • **Blackmail** - A new phishing email has been found in the US and Australia, where fraudsters are blackmailing victims, claiming they will infect their family with the coronavirus if they do not pay a fee. They claim to know everything about the victim and may even display a password that has been leaked in a data breach, that the recipient would be familiar with. These emails have been compared to popular phishing email tactics like those threatening to expose indecent images of the victim. However, this email attack goes further by threatening the lives of the recipient's family. If you receive an email like this, you should forward it on to the NCSC phishing email account (report@phishing.gov.uk) and contact Police Scotland on 101 **For more information and what to do to reduce the risk view Cyber Resilience Notice - 7 May 2020**

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
05 May 20	**City of London Police -** What scams are we seeing?		**The majority of reports are still related to online shopping scams where people have ordered protective face masks, hand sanitiser, COVID-19 testing kits, and other products, which have never arrived.** **Other frequently reported scams include:** • Victim receives an email from a trusted source, such as another employee or a supplier, instructing them to make a payment to a different account than usual due to the outbreak. Victim changes the payment details. The new account is actually controlled by the suspect who is impersonating the trusted source. • Suspect advertises a pet online (puppy or kitten) and uses the outbreak as a reason the victim can't come and see the animal. The suspect sends photos and persuades the victim to make a payment in advance. The suspects will often try to get the victim to pay additional unforeseen costs (insurance, vaccinations) after they've made the initial payment but never provide the pet. NOTE: Action Fraud will be issuing an alert on this scam tomorrow • Victim tried to apply for a government grant to assist their business during the outbreak but was informed their business had already received a grant and were therefore not eligible for any more financial assistance. The victim did not make this initial application and does not recognise the account the payment was made to. • Suspects are incorporating the coronavirus pandemic into push payment frauds and using the outbreak to convince victims to speak with the suspect on the phone, saying the banks are closed etc.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			Phishing/smishing trends • **Bitcoin investment -** City of London Police continue to receive a high number of reports about emails advertising investments in Bitcoin platforms that claim to "take advantage of the financial downturn" and can help people recover from bankruptcy. A link is provided in the email which claims to take recipients to a website that explains how Bitcoin trading platforms work. This link has two main threats; one for phishing and one for malware, where the suspect is trying to steal credentials and/or get the recipient to download a virus. • **COVID-19 Government grants** - Emails purporting to be from government state the recipient can get a free evaluation for emergency COVID-19 tax relief. The emails are personalised to the recipient and contain a malicious link. • **Antigen testing** - Emails advertising a COVID-19 'prick test for antigens' which spoof the email address of a genuine UK medical supply retailer. Links within the emails are confirmed as phishing.
05 May 20	**Investment Fraud**	UK Action Fraud	An Action Fraud spokesperson said: "Fraudsters will use any opportunity they can to take money from the public. This includes exploiting tragedies and global emergencies. "While the pandemic has created opportunities for criminals to exploit, reports of fraud to Action Fraud have not increased during the COVID-19 outbreak. Reports of investment fraud have also not increased. However, it can take some time before an investment scam is spotted by its victims. We are monitoring this, and all crime types, very closely.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			"It is likely that criminals will continue to attempt to exploit the impact of COVID-19 on the economy and people's personal finances, as they did after the financial crisis in 2008. This could lead to a rise in fraudulent investment schemes, so we would advise people to remain vigilant at this time. If you are thinking about making an investment, please check the FCA's register to make sure the company is regulated. If you deal with a firm or individual that isn't regulated, you may not be able to get your money back if something goes wrong." Top tips for spotting an investment scam: • You're contacted out of the blue by phone, email or social media about an investment opportunity; • You're pressurised into making a decision with no time to consider the investment; • You're offered a high return on your investment with apparently little or no risk; # • You're told the investment opportunity is exclusive to you.
30 Apr 20	**Trading Standards Scotland** latest scams across Scotland.	Scam Share - Bulletin 7	This Bulletin highlights: • **Ticket Refunds -** Consumers across Scotland have been struggling to obtain refunds for cancelled shows and events, with many companies offering rescheduled dates or vouchers instead of full refunds. Any companies who are registered with the Society of Ticket Agents and Retailers (STAR) must refund the face value of a ticket if an event is cancelled; however many smaller companies are not registered with STAR and will have their own refund policies. • **Business Scams -** The Highland Council has warned local businesses about scam emails which inform the business that their grant application has been processed and that they will receive a payment soon. The email provides bogus

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			contact details to use if the payment is not received, in the hope that companies will call and provide their financial details. A number of similar scams have been reported across the UK, with fraudsters contacting businesses by email, text or phone to tell them that they qualify for a particular grant or tax refund. • **Charity Scams -** There have been reports of calls claiming to be from the 'Corona Charity Fund' which make claims about the expected death toll in UK and ask for a donation to charity. As well as cold calls, there are numerous websites posing as charities who are fundraising to help victims of COVID-19 or to support health services. Consumers are also receiving emails and visits from fraudsters posing as charity workers. Emails may seem genuine, with official-looking Government or NHS logos and seek to exploit the public's desire to support NHS staff. They may ask for donations to help purchase medical supplies or to fund mental health support initiatives for NHS staff. Be particularly wary of bogus charity emails which request donations via bank transfer or gift card - genuine charities will not ask for donations in this way. • **Unapproved Antibody Testing Kits -** The national coordinator of the UK COVID-19 testing programme has warned organisations and individuals against the purchase of unapproved antibody testing kits, used to detect whether people have had the virus and are now immune. There are currently no reliable antibody testing kits available to purchase which have been approved for public use. People are being warned that using unapproved tests could provide inaccurate results, which could put those tested and people around them at risk. As soon as a reliable testing kit becomes available, this will be announced by the Government. • **Unfair Business Practices -** As of 19 April, the Competition and Markets

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			Authority (CMA) had received around 21,000 complaints related to COVID-19, mostly focused on price rises for in-demand products and cancellations or refunds. They are writing to businesses about price rises and will this week set out further steps on how they intend to tackle issues surrounding cancellations and refunds. Consumers can use their online reporting tool to report a business they believe is behaving unfairly during the COVID-19 outbreak. • **'Clone Firms'** - Debt charity Step Change have issued a warning about 'clone firms'. These are fake websites who use altered versions of genuine debt advice charities' names in order to convince people that they are legitimate and trick them into providing personal and financial details. • **Travel Cancellations -** There remains a great deal of uncertainty around travel and accommodation amendments and refunds – View Bulletin 7 for the most recent guidance and advice. **For more information and What to Do view Scam Share - Bulletin 7**
30 Apr 20	**Scottish Government Cyber Resilience Unit** - Sharing important information and guidance on COVID-19 related scams.	Cyber Resilience Notice - 30 April 2020	**Zoom Update** Important issues have been raised about encryption and who keeps records or can listen in to calls. To help meet privacy obligations for their customers Zoom report that they are introducing a new encryption method and the ability to report users. They have also increased the minimum password length for meetings. You can read more about Zoom 5.0 and how to update your version. **NCSC Guidance on Video Conferencing:** • Video Conferencing services: using them securely - guidance for individuals and families about the use of video conferencing software.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			• Video conferencing services: guidance for organisations – advice about how businesses can use video conferencing safely and securely. • Video conferencing: new guidance for individuals and organisations (BLOG POST) – content introducing the two new pieces of guidance above (refers to schools and National Crime Agency advice). **NCSC Guidance for schools and colleges (online/remote learning and teaching** Now, more than ever, schools are relying on online technologies for learning and teaching as well as admin tasks. All staff can play a role in keeping online services (and the information they access) secure, safe and available. NCSC have produced some Practical Tips for school and college staff to help them understand what cyber security is, how it's relevant and what steps they can take to improve their school's resilience when faced with cyber threats. The Blog that sits alongside this is also very helpful. **Information and guidance for young people** • Young Scot DigiAye - Tips for young people on how to be more cyber resilient • Young Scot DigiKnow - Want to start a career in cyber security? This guide is filled with fun ways to learn digital skills and alternative ways to get into the industry, as well as info on how to stay safe online • Young Scot Learning resources - for anyone working with young people, including resources relating to staying safe online **Get Safe Online**

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			Get Safe Online '<u>Safe email</u>' campaign went live on 1 May 2020. The campaign focuses on advice specific to the COVID-19 outbreak, including identifying phishing emails and safe home working. **Trending Topics:** • **Fake NHS website** - A hoax copy of the NHS website has been discovered. The website includes harmful links to COVID-19-related health tips. Once these links are clicked on, a pop-up box appears asking visitors to save a file called 'COVID19'. If saved, the malware it contains can steal passwords, credit card data, cookies from browsers, crypto wallets, files and screenshots. • **COVID-19 Testing scam -** Reports are being received from the US of a new SMS scam claiming, 'someone who came into contact with you has tested positive for COVID-19'. Attackers have deployed a phishing campaign against remote workers using Skype, luring them with phishing emails with fake notifications from the service. The social engineering in this campaign is refined enough to make many people access the fraudulent login page and provide their credentials. Furthermore, the username is automatically filled in, which only helps reduce suspicion. All the victim has to do is type in their password and the attacker gets it automatically. • **Retailers** - Police have issued warnings of ongoing phishing emails and WhatsApp messages claiming to be from well-known retailers (such as Morrisons, Tesco and Heineken) offering free goods or vouchers. If you get a message like this, don't click on the links and don't share any personal or financial information. **For more information and advice view <u>Cyber Resilience Notice - 30 April 2020</u>**

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
23 Apr 20	**Trading Standards Scotland** latest scams across Scotland.	Scam Share - Bulletin 6	This Bulletin highlights: • **Travel Cancellations -** 50% of complaints by Scottish consumers logged last week were related to travel and accommodation. A study by consumer body Which? has discovered that 20 of the UK's biggest airlines and holiday companies are failing to meet their legal requirements by either refusing to issue refunds to customers or by offering vouchers or credit notes. Customers are being advised not to accept vouchers as these will not be ATOL-protected and may prove worthless if the company collapses. Under EU law, travel companies must refund customers within 14 days if their package holiday is cancelled. • **Mobility Aids Scams -** There were reports from consumers, one of whom is in their 90s, in South Lanarkshire this week about cold callers who claimed to work for Stannah Stairlifts and phoned to arrange an annual service. When the engineer arrived at the elderly consumer's property, he asked her to stay in her living room to adhere to social distancing rules while he supposedly checked her stairlift. • **Netflix Scam -** Scammers are taking advantage of the huge surge in the numbers using online streaming services due to the COVID-19 lockdown (including a 32% increase in paid subscriptions to Netflix) by sending fake emails claiming to be from Netflix asking users to click a link to update payment details. The link leads to a fake payment page with Netflix branding, where you will be asked to enter personal and card details. • **Misleading Adverts for IV Drips -** The Advertising Standards Authority (ASA) have published three rulings involving businesses who offer intravenous (IV) drip treatments and which claimed to prevent or provide treatment for COVID-19. All three businesses were in breach of the advertising rules and the ASA fast-tracked

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			these investigations as part of their focus on tackling businesses and advertisers who are using this pandemic to profit from people's fears and anxieties. • **Hand Sanitiser: Official Guidance -** The Office for Product Safety and Standards (OPSS) have updated their guidance for businesses on placing hand cleaning and sanitising products on the market and regulations for manufacturing personal protective equipment (PPE). The latest blog post from Vistalworks highlights the potential dangers of homemade hand sanitiser. • **Volunteer Shopping Cards -** Several supermarkets have now introduced 'volunteer shopping cards' to help those self-isolating to avoid frauds. Consumers who are unable to visit shops themselves can purchase a card online (similar to a regular voucher) and send the link to a volunteer or print a barcode and leave it in a safe place. The volunteer can then purchase groceries for them without having to exchange a physical payment or card/bank details. • **Pension Scams -** The Association of British Insurers (ABI) has warned against 'pension panic' due to COVID-19. **For more information and What to Do view TSS Scam Share - Bulletin 6**
23 Apr 20	**Scottish Government Cyber Resilience Unit** - Sharing important information and guidance on COVID-	Cyber Resilience Notice - 23 April 2020	**National Cyber Security Centre** - have launched the new Cyber Aware campaign promoting behaviours to mitigate cyber threat. The cross-governmental 'Cyber Aware' campaign, offers actionable advice for people to protect passwords, accounts and devices. You can find out more about what NCSC have launched recently here. This includes new guidance for individuals and organisations using online video conferencing. **Tips for spotting tell-tale signs of phishing (fake emails)** - Spotting a phishing email is becoming increasingly difficult, and many scams will even trick computer

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
	19 related scams.		experts. However, the Cyber Resilience Notice - 23 April 2020 provides some common signs to look out for. **Scottish Businesses Care: COVID-19 and counterfeit goods -** In this webinar, the panel discuss the rise of counterfeit goods during the COVID-19 pandemic, hosted by Rachel Jones of SnapDragon Monitoring. https://youtu.be/z6GWudEa8Qo **New Scottish Government Guidance For Home Learning –** This new guidance is aimed at pupils, parents and teachers, which makes reference to digital learning, with a focus on safety, security, privacy and safeguarding. This complements earlier guidance published by The General Teaching Council Scotland relating to online engagement by education professionals. **Google** - The BBC have reported that scammers are sending 18million hoax emails about COVID-19 to Gmail users every day, according to Google. The tech giant says the pandemic has led to an explosion of phishing attacks in which criminals try to trick users into revealing personal data. **Tesco Vouchers -** There have been reports about fake emails that appear to be from Tesco. The email states that the supermarket is offering free vouchers. The link in the email leads to a phishing website that looks like the genuine website that is designed to steal login credentials as well as personal and financial information. **Netflix Scam** - The cybersecurity firm BrandShield have noted that since January 2020, 639 fake domains containing the word "Netflix" have been registered. These are being used to steal users' credentials, money, or even to spread malware onto users devices. Users should be cautious and only enter credentials into the legitimate Netflix website (Beware of phishing scams in other brands, for example TV licencing, BT Sport, Virgin Media, Amazon and a general increase in scams for other brands that have been around for a while).

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			Sextortion Scam - The scam involves emails being sent to people with the suspect claiming to have video footage of the recipient visiting an adult website. The suspect is then demanding payment in bitcoin, threatening that failure to do so will result in the video being published. This is known as sextortion, an example of a phishing attack. **For more information and what to do to reduce the risk view Cyber Resilience Notice - 23 April 2020**
16 Apr 20	**Trading Standards Scotland** latest scams across Scotland.	Scam Share - Bulletin 5	This Bulletin highlights: • **Online Shopping -** When shopping online, carry out some research before purchasing from sellers or companies you are not familiar with. The National Cyber Security Centre has detailed advice to help consumers shop safely online. Solicitors Austin Lafferty have published an article this week offering practical advice on how to shop safely online and avoid scams. If you decide to go ahead with the purchase, use a credit card if you have one, as most major credit card providers insure online purchases. • **Online Quizzes -** Consumers are being urged by the Chartered Trading Standards Institute (CTSI) to be wary of online quizzes related to COVID-19. These quizzes may appear to be testing your knowledge about the spread of the pandemic but ask for a range of personal details which could be used to commit financial fraud or identity theft. • **Misleading Information –** Update on Bulletin 4. • **Doorstep Scams -** Update to Bulletin 4. • **Misleading Advertising -** The Advertising Standards Authority (ASA) want to stop businesses and advertisers from using the COVID-19 pandemic to profit from people's fears and anxieties. Adverts which have potentially harmful,

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			misleading, or irresponsible information about COVID-19 can be reported to the ASA using their new form. Find out more on their website. • **Unfair Business Practices -** The Competition and Markets Authority (CMA) has launched an online reporting tool to make it easier for consumers to report a business they believe is behaving unfairly during the COVID-19 outbreak. • **IPTV (Illicit Streaming) -** If you are stuck at home with nothing to do, it may be tempting to buy a cheap illegal streaming service or device. These illegal devices and platforms are one of the main sources of malicious software and those who sell them are unlikely to protect your personal and financial data. • **Fake Medical Products -** A pharmacist and a surveyor were arrested this week on suspicion of illegally selling testing kits for COVID-19. In a separate case, a website which was sending phishing emails to try to sell non-existent PPE has been taken down by the National Crime Agency. • **Scottish Citizens Stranded Abroad -** Advice Direct Scotland have updated the information on their COVID-19 consumer website with advice and recommendations for Scottish citizens who are stranded abroad. • **Temporary Financial Support -** The Financial Conduct Authority (FCA) have introduced new temporary measures to quickly support users of credit products such as loans, credit cards and overdrafts who are facing changing financial circumstances due to COVID-19. Find out more on their website. If you've been offered a personal loan via an online advert or unsolicited email, you should check whether the lender has been authorised by the FCA on their register. • **Fire Safety -** Be careful when buying electrical devices online: **counterfeit** products may not conform to EU or UK electrical safety regulations and research

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			by Electrical Safety First shows that 1 in 10 Britons have experienced a fire or electric shock after using fake electrical products purchased online. **For more information and What to Do view TSS Scam Share - Bulletin 5**
16 Apr 20	**Scottish Government Cyber Resilience Unit** - Sharing important information and guidance on COVID-19 related scams.	Cyber Resilience Notice - 16 April 2020	**Scottish Business Cares -** The do's and don'ts of video conferencing. This webinar recording investigates video conferencing and how to do it securely. Learn how easy it is to protect your meetings with ethical hackers; Declan Doyle, Jess Amery and Moe Keir. https://youtu.be/LITHJZypIpA **Zoom Bombings** - There have been cases globally of video conferencing broadcasts and meetings being hijacked by malicious users including a recent incident where obscene content was broadcast during an online swimming workout aimed at children in Scotland. This event, along with other events that are open by design are vulnerable to being hijacked as anyone can join them. **Zoom Account Hacked** - Other trusted sources have reported that up to 500,000 hacked Zoom account passwords are available on the dark web. **Patching and security updates -** Research has revealed that 12% of vulnerabilities were exploited within one week of patch issuance and 27% within one month. This makes the impact of these exploits entirely preventable by patching. You are in a race to patch against someone wishing to exploit the vulnerabilities. **Child Online Sexual Abuse -** Children and young people are spending a lot more time online for learning and socialising during the Covid-19 Pandemic, and with parents, carers and guardians working from home, children are allowed more screen time than usual. **Young Scot** is stepping up efforts to promote their vast range of resources and

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			materials to support young people to be more resilient online through their communications channels on Twitter, Facebook, Snapchat, Instagram and TikTok. The Scottish Government is developing a Parent Club campaign on channels including TV, radio, digital and social media, offering practical advice and support across the breadth of challenges parents are facing during this time, including online safety. **For more information and what to do to reduce the risk view Cyber Resilience Notice - 16 April 2020**
09 Apr 20	**Trading Standards Scotland** latest scams across Scotland.	Scam Share - Bulletin 4	This Bulletin highlights: • **Fake Shopping Vouchers -** The Chartered Trading Standards Institute (CTSI) this week received evidence of a shopping voucher scam related to the COVID-19 pandemic. • **Fake Texts from Phone Providers -** Saying that a payment has been declined and asking them to click on a link to update their payment details. • **5G: Misleading Information -** Following vandalism of mobile phone masts across the country, Ofcom has this week issued a statement emphasising that there is NO relationship between 5G mobile signals and COVID-19. • **Unfair Pricing -** The Competition and Markets Authority (CMA) has this week launched a new online reporting tool to make it easier for consumers to report a business they believe is behaving unfairly during the COVID-19 outbreak. • **Pension Scams -** The Pensions Regulator (TPR) and the Financial Conduct Authority (FCA) have warned that savers' fears about the impact of the COVID-19 pandemic on markets and personal finances may make them more vulnerable to scams.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			• **Fake Products Online -** Vistalworks have recently updated their online checker to include baby products, such as formula, milk and nappies as well as a variety of so-called 'cures' for COVID-19. • **Doorstep Scams -** Update to Bulletin 3. • **Cancellation Rights -** Update to Bulletin 3. • **Scottish Illegal Money Lending Unit -** The Financial Conduct Authority (FCA) have this week proposed new temporary measures to quickly support users of credit products such as loans, credit cards and overdrafts who are facing changing financial circumstances due to COVID-19 Find out more on their website. • **Find Trusted Information on COVID-19 -** Update to Bulletin 3. **For more information and What to Do view TSS Scam Share - Bulletin 4**
09 Apr 20	**Scottish Government Cyber Resilience Unit** latest scams across Scotland.	Cyber Resilience Notice - 9 April 2020	**Smishing/Phishing** - Fake texts messages and emails appearing to be from a trusted source. Latest scam text messages to look out for include those that: • Claim to link you to a GOV.UK website to claim COVID-19 relief payments, council tax or business rate 'holidays' or similar. • HM Government asking for donations to the NHS during the COVID-19 outbreak. • Suggest you have been seen leaving your home on multiple occasions in breach of lock-down laws and levying 'fines'. • Offering "health supplements" or Personal Protective Equipment supplies that falsely claim to prevent you becoming infected with COVID-19.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			• Appear to come from your bank and relate to mortgage holidays or other financial support (business or consumer). Be wary of any texts you receive, even if it appears to come from an organisation you know and trust. Don't follow links in text messages or phone any numbers provided. If you believe a text message is genuine and require more information, contact the organisation via their website by typing their genuine web address into your browser. **Home Working** - The National Cyber Security Centre (NCSC) have produced advice and guidance to help individuals and businesses who are working from home to stay safe online. How to make sure your organisation is prepared for an increase in home working, and advice on spotting coronavirus (COVID-19) scam. **Web Conferencing** - Communications platforms (such as Zoom and Microsoft Teams) for online meetings are becoming popular given the need for home based working. Malicious cyber actors are taking advantage of this and are hijacking online meetings that are not secured with passwords or that use unpatched software. **For tips against online meeting hijacking and further information and advice view Cyber Resilience Notice - 9 April 2020**
08 Apr 20	**West Mercia Police -** What scams are we seeing?	Online Safety and Security	**The majority of reports are still related to online shopping scams where people have ordered protective face masks, hand sanitiser, COVID-19 testing kits, and other products, which have never arrived.** **Other frequently reported scams include:** • Suspect impersonating the government and notifying the victim they were due a payment/rebate.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			• Suspect incorporating the COVID-19 epidemic into push payment frauds. • Suspect asking for a donation to tackle COVID-19, normally via email or pretending to be from a charity which is assisting vulnerable people during the outbreak. • Suspect calling purporting to be victim's bank, saying account was compromised/there had been unusual activity. Victim advised to open new account/transfer money there and then. Victim told they should not visit their branch because of COVID-19. • Suspect persuades victim to make an advanced payment for a rental property. The suspect uses the outbreak as the reason for the victim being unable to view the property. The property does not exist, or the suspect is not in a position to rent it. • Suspect uses COVID-19 as a hook for offering employment. Victim is persuaded to pay an advanced fee for vetting/qualifications to get them the job which ultimately does not exist.
02 Apr 20	**Trading Standards Scotland** latest scams across Scotland.	Scam Share - Bulletin 3 OfCom	This Bulletin highlights: • **Cyber Security** - With most of the country now working from home or in isolation, it is more important than ever to be aware of cyber security - Stay Safe Online. • **Email/Text Scams:** ➢ Ofcom has published advice for consumers on dealing with phone and text scams related to COVID-19. In recent days, there have been several scam texts which appear to be from the UK Government offering money to all residents. ➢ An email saying that you have been in contact with someone who is infected with COVID-19.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			➢ Email or text supposedly from Netflix saying that your account has been suspended. ➢ Email supposedly from the World Health Organisation (WHO) asking you to click on a link or download information about COVID-19. • **Charity Scams** - There are numerous new websites posing as charities who are fundraising to help victims of COVID-19 or to support health services. Consumers are also receiving emails, phone calls and visits from fraudsters posing as charity workers. • **Fake Products Online** - There are currently no products or supplements available to purchase which have been approved by the UK Government for use in the prevention or cure of COVID-19. Any products or cures advertised may be fake and potentially dangerous. • **Doorstep Scams** – An elderly couple in Moray were visited by someone posing as a member of the Council, with a legitimate-looking Moray Council ID badge, who offered to buy food for them. They handed her cash, but she did not return with any groceries. • **Cancellation Rights** - Many consumers have been seeking advice and information about their cancellation rights. • **Loan Sharks** – Update to Bulletin 2. • **Find Trusted Information on COVID-19** - Update to Bulletin 2. **For more information and What to Do view TSS Scam Share - Bulletin 3**

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
31 Mar 20	**Universal Credit Scam**	Humberside Police Online Fraud	Secretary of State for Work and Pensions Therese Coffey: "We know cyber criminals and fraudsters are despicably attempting to exploit opportunities around coronavirus. DWP will never text or email asking for your personal information or bank details. Anyone who thinks they have been a victim of fraud should report it to Action Fraud, and notify DWP, as soon as possible." **Action Fraud Advice** • Take a moment to think before parting with your money or information, especially if the request has come from a cold call, or unexpected text or email. Could it be fake? Do you know or trust the person it's come from? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you. Take your time to discuss what is being asked of you with friends or family. • The police, or your bank, will never ask you to withdraw money or transfer it to a different account. They will never ask you to reveal your full banking password or PIN. • If you receive an unexpected text or email asking for personal or financial details do not click on the links or attachments. Ensure you have the latest software and application updates installed on all your devices. • If you believe you have been a victim of fraud, please report this to (Police Scotland on 101).
30 Mar 20	**COVID-19 related scams**	Get Safe Online	• Be wary of approaches from supposed travel agents, tour operators, airlines, cruise companies, insurance companies or compensation firms promising to arrange travel, accommodation or event entry refunds: they may well be fraudulent. If in doubt, call the company you have been dealing with, on the phone number you know to be correct. These approaches can take the form of emails,

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			texts, social media posts, direct messages, online advertisements and phone calls. • Be wary of ads for products such as facemasks, hand sanitiser, vaccines, cures and hard-to-get goods, as they could be for non-existent products. Never pay by bank transfer, and where possible pay by credit card as doing so provides additional protection. • Don't click on unknown links in emails, texts or posts, or email attachments. They could link to websites that capture your passwords and other confidential details or cause a malware infection, both of which can result in financial or identity fraud. They could also link to adult, hate, extremist or other content.
27 Mar 20	**HMRC** related phishing emails and bogus contact	HMRC	Details of HMRC phone, email and online scams are on their website: • **Email Scams** – Campaign telling customers they can claim a tax refund to help protect themselves from the COVID-19 outbreak. • **SMS Scams:** ➢ Telling customers they can claim a 'goodwill payment'. Do not reply to the SMS and do not open any links in the message. ➢ States you will be fined £250 for leaving the house more than once. The message asks recipients to call an 0800 telephone number to appeal. Do not reply to the SMS or call the phone number listed. • **Tax Refund and Rebate Scams** - HMRC will never send notifications by email about tax rebates or refunds. Do not: visit the website; open any attachments; disclose any personal or payment information. Fraudsters may spoof a genuine email address or change the 'display name' to make it appear genuine. If you are unsure, forward it to HMRC and then delete it.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			• **Text Messages** - HMRC will never ask for personal or financial information when they send text messages. Do not reply if you get a text message claiming to be from HMRC offering you a tax refund in exchange for personal or financial details. Do not open any links in the message. Send any phishing text messages to 60599 (network charges apply) or email phishing@hmrc.gov.uk then delete it. • **Bogus Phone Calls** - HMRC is aware of an automated phone call scam which will tell you HMRC is filing a lawsuit against you, and to press one to speak to a caseworker to make a payment. HMRC can confirm this is a scam and you should end the call immediately. • **WhatsApp Messages** - HMRC will never use 'WhatsApp' to contact customers about a tax refund. If you receive any communication through 'WhatsApp' saying it is from HMRC, it is a scam. Email details of the message to phishing@hmrc.gov.uk then delete it. • **Social Media Scams** - HMRC is aware of direct messages sent to customers through social media. A recent scam was identified on Twitter offering a tax refund. These messages are not from genuine HMRC social media accounts and are a scam. • **Refund Companies** - HMRC is aware of companies that send emails or texts advertising their services. They offer to apply to HMRC for a tax rebate on your behalf, usually for a fee. These companies are not connected with HMRC in any way. You should read the 'small print' and disclaimers before using their services.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
26 Mar 20	**Trading Standards Scotland** latest scams across Scotland.	Scam Share - Bulletin 2	This Bulletin highlights: • **Email Scams** – About entitlement to free school meals; Government are offering everyone a basic wage; Government has issued a payment to all UK residents; text or call supposedly from the NHS asking for donations to fund a cure for COVID-19; claiming to be from various charities asking for donations. • **Bank Fraud** - Caller pretending to be from bank, saying that the bank was closed due to COVID-19 and asking him to verify his account details in order to pay an outstanding bill. The consumer had £4,000 taken from their bank account. • **Fake Products Online** - Products advertised online which claim to cure or prevent Coronavirus. • **Doorstep Scams** – Update to Bulletin 1. • **Community Support** – By following five simple guidelines, both those in need of help and those wishing to provide help can ensure that they stay safe. • **Unfair Pricing** - Update to Bulletin 1. • **Loan Sharks** - The COVID-19 outbreak has led many people across Scotland to find themselves in a financially vulnerable position, either through losing their jobs or through uncertainty about payments for rent, utilities and basic necessities. • **Find Trusted Information on COVID-19 -** Update to Bulletin 1. **For more information and What to Do view TSS Scam Share - Bulletin 2**
19 Mar 20	**Trading Standards Scotland** latest scams across	CFS Intelligence Alert: 12 2019/20 Scam Share - Bulletin 1	This Bulletin highlights: • **Fake Products Online -** Fake testing kits to homemade hand sanitiser and from 'miracle cures' to IV drips. • **Doorstep Scams -** Reports about rogue traders cold calling households and offering to spray paths and front doors to get rid of bacteria. Others have reported

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
	Scotland.		fraudsters posing as NHS staff and offering to help people with their shopping in return for payment or trying to get donations to fund a 'vaccine'. • **Email Scams -** Offering a tax refund; offering a cure for the Coronavirus; claiming to be from the World Health Organisation (WHO); claiming to be from your bank asking you to update your account security information. • **Holiday/Travel Scams -** Emails and phone calls claiming to be from travel agents, tour operators, insurance companies and compensation firms. • **Unfair Pricing -** Unscrupulous traders, both online and in retail outlets, have been inflating prices on in-demand goods such as hand sanitisers, toilet rolls and face masks. • **Find Trusted Information on COVID-19 -** Misleading stories being shared online and through social media. Many of these stories can cause panic and distress, particularly to vulnerable people, and can make people more susceptible to being scammed. **For more information and What to Do view TSS Scam Share - Bulletin 1**
18 Mar 20	**Cybercriminals - Social media scams** Advice to help NHS	CFS Intelligence Alert: 10 2019/20 UK Action Fraud	• **Social Media Scams -** A fake WhatsApp message appears as if they have been sent by someone in your contacts – such as a friend or family member. **For more information visit UK Action Fraud website**. • **Beware of Gift Cards** - Links are shared via social media to a giveaway of free

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
	members of staff to protect themselves against increased social media scams	Sophos	gift cards. Clicking on the link takes you to a third-party website, encouraging you to sign up for another service before you can access the gift card. The scammers are earning affiliate cash by driving traffic to these websites. **Find out more by visiting Sophos website.**
18 Mar 20	**Cyber scams** Advice to help NHS members of staff to protect themselves against increased cyber scams	CFS Intelligence Alert: 10 2019/20	• **Bait and Switch Online Scams** - If it sounds too good to be true, it probably is. This offer is designed to lure you in, but instead of getting something too good to be true, you get a very different deal indeed (the "switch"). It can be an inferior product or service, or you get what is advertised but at a much higher price. Either way, each instance is a clear case of fraud and is punishable by law. • **Delivery Problem -** It can be difficult to keep track of a large number of online orders. However authentic the email, and the accompanying page appear, do not trust it. An email might pretend to be FedEx, DHL, or UPS and ask you to download an attachment. Don't. Simple as that. You could be downloading ransomware, or a virus that tracks your activities.