Counter Fraud Services

Protecting Resources
Delivering Solutions

NHS National Services Scotland

Rolling COVID-19 Intelligence Alert No. 14 - 3 August 20

OFFICIAL-UNMARKED

NHSSCOTLAND CFS COUNTER FRAUD SERVICES

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, 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. A glossary of terms is provided at the end of the document.

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. This book should be seen as a general guide to the many scams currently operating in the UK and increases awareness of these scams and teaches you some easy steps that you can take to protect yourself and others.

The Little Book of Big Scams Business Edition offers fraud prevention advice to safeguard your business against fraudulent acts whilst complying with the law and relevant regulations. This advice is for small and medium size enterprises but is relevant to larger organisations including the NHS and the wider public sector.

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

To report a crime call **Police Scotland on 101** or in an emergency 999.

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**
28 Jul 20	**Audit Scotland –** COVID-19 Emerging Fraud Risks	https://www.audit-scotland.gov.uk/uploads/docs/report/2020/briefing_200723_covid.pdf	NHS Scotland Counter Fraud Services supported Audit Scotland to prepare this briefing which: • Sets out a range of fraud risks emerging from the COVID-19 crisis; • Provides guidance to public bodies to help reduce these risks; • Raises awareness of these new fraud risks with public bodies; • Supports public bodies in identifying and managing these risks to ensure that sound governance and controls are in place.
23 Jul 20	**NHS Board DoF Email Spoofing Scam**	CFS Intelligence Alert: 05 2020/21	This Alert highlighted a recent unsolicited email approach, purporting to have been authorised and sent by a NHS Board Director of Finance. The email was for payment of an outstanding invoice for £23,945. The company purporting to have issued this email is a genuine company, although it is not one that the Board have had any previous dealings with.
24 Jun 20	**Council Purchase Email Spoofing**	CFS Intelligence Alert: 04 2020/21	This Alert highlighted unsolicited email approaches, purporting to have been issued from a regional Council creditor department. This is commonly referred to as email spoofing. It is how spammers send emails that look like they have originated from genuine email accounts. The email "From" header appears legitimate, when in fact the genuine owner of the email account knows nothing about it.
16 Jun 20	**Attempt Bank Mandate (Account Takeover) Fraud**	CFS Intelligence Alert: 03 2020/21	An email scam was received from a fraudster purporting to be the managing director of Abellio ScotRail Ltd. The email was sent to an NHS staff member requesting copies of initial contracts / award letter and previous invoices last issued to the Board. The email also noted that due to COVID-19 there has been a change in their contract payment accounts and that Abellio had been forced to change banks due to a better management of cash flow. Abellio ScotRail Ltd have confirmed this is a scam.

Table 1: Protecting NHS Scotland from fraud during COVID-19			
Date	**Topic**	**Links to sources**	**Advice and Guidance**
04 Jun 20	**Scottish Government Cyber Resilience Unit -** Sharing important information and guidance on COVID-19 related scams.	Cyber Resilience Notice - 04 Jun 2020	**Returning to work** Over the coming weeks many people will be returning to work and switching on computers and opening email inboxes for the first time in months. But as we do that what are some of the cyber security considerations we should be thinking about? Police Scotland recommend that you: • **Install updates** – Consider running an update to see what patches, or updates, are available for your system as these may contain vital security improvements. Make sure to have an up-to-date back-up of your system in case you need it. • **Phishing Emails** - Be on the lookout for any phishing emails. Do not click on any links in a suspicious email, report it to your IT department or provider and remember to forward it to the NCSC's Suspicious Email Reporting Service – report@phishing.gov.uk. • **Mandate fraud** -You may also find some "urgent" invoices requesting immediate payment in your inbox. Using social engineering cyber criminals can learn who you do business with and then send you fake invoices in that company's name. We call this "mandate fraud" and some of the tell-tale signs are an urgency with the request and also a request to change bank details. If you are unsure then never immediately pay and use a trusted telephone number to contact the company and confirm the request. **For more information and what to do to reduce the risk view Cyber Resilience Notice - 04 Jun 2020**
28 May 20	**COVID-19 Business Grant Scam Emails**	NAFN Data and Intelligence Services	A number of national companies have been targeted by fraudsters making fraudulent enquiries and applications for COVID-19 Retail, Hospitality and Leisure grants. The fraudsters are sending what appear to be legitimate requests for property details,

Table 1: Protecting NHS Scotland from fraud during COVID-19			
Date	**Topic**	**Links to sources**	**Advice and Guidance**
			reference numbers and extended retail discounts. The names used in the emails are either unknown to the businesses or legitimate (current/retired) employees added to fake email domains. All domains appear to have been registered in April and May 2020. Members confirm the number of businesses targeted is growing.
28 May 20	**Scottish Government Cyber Resilience Unit -** Sharing important information and guidance on COVID-19 related scams.	Cyber Resilience Notice - 28 May 2020	**CPNI – Staying secure during COVID-19** - The Centre for the Protection of National Infrastructure (CPNI) have created a resource page to help organisations to stay secure during COVID-19. This includes guidance from CPNI and NCSC as well as a 'living' campaign which can be adapted by workplaces to aid them in opening and operating as safely and securely as possible in the coming weeks and months. There is also guidance on protective security and managing risks as well as guidance on personnel security during a pandemic and on insider threats. **For more information and what to do to reduce the risk view Cyber Resilience Notice - 28 May 2020**
26 May 20	**Scottish Business Resilience Centre**	Scammers Are Posing As The NHS Cervical Screening Programme	Reports of scams circulating where scammers are posing as the NHS. The National Cervical Screening programme involves sending a text to individuals to remind them to book an appointment. These have been put on hold during the lockdown period in the UK. Several individuals have reported receiving texts that look like they come from the NHS, but upon closer inspection, these text messages are from scammers. Individuals have been advised that if they have any concerns, they should contact their local GP to check authenticity of messages received.
07 May 20	**Scottish Government Cyber Resilience Unit** - healthcare	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**

Table 1: Protecting NHS Scotland from fraud during COVID-19			
Date	**Topic**	**Links to sources**	**Advice and Guidance**
	bodies at risk of malicious cyber activity		**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	**Scam Share 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 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.

Table 1: Protecting NHS Scotland from fraud during COVID-19			
Date	**Topic**	**Links to sources**	**Advice and Guidance**
			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.**
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

Table 1: Protecting NHS Scotland from fraud during COVID-19			
Date	**Topic**	**Links to sources**	**Advice and Guidance**
			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 Europol 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**
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**
30 Jul 20	**Trading Standards Scotland** latest scams across Scotland	Scam Share - Bulletin 20	This Bulletin highlights: • **Fake Brands on Social Media -** Since the beginning of the Covid-19 pandemic, we have reported on the rise of fake websites and social media adverts as the counterfeit trade moves increasingly online. Now, social media influencers are being warned that they may be unwittingly promoting fake brands. This video from BBC News shows how some influencers with up to 2 million followers are promoting fake brands through Facebook and Instagram. • **Ongoing Advice: Travel Insurance -** Following the removal of Spain from the list of countries who are exempt from quarantine restrictions from 26 July, Advice Direct Scotland have published guidance for those who are planning on travelling to Spain and those who are returning to Scotland and are required to self-isolate for 14 days. Advice Direct Scotland also have a guide to flight and holiday refunds to ensure that you are aware of your consumer rights when things don't go to plan. • **Ongoing Advice: Test and Protect Scams -** Since the launch of the Test and Protect system, there have been several reports of scammers posing as contact tracers and asking people to make payments for tests or asking for financial information, social media logins or passwords. NHS Scotland will now call from a single national number: 0800 030 8012. They will introduce themselves, state the reason for their call and address you by your name. If they do not know your name, they are not a genuine contact tracer. • **Ongoing Advice: PayPal Scams -** Action Fraud have issued a warning about PayPal scams after they received over 1,000 reports of fake PayPal emails in just one day. The scam email claims that your account has been limited due to a policy violation and asks you to click on a link to verify your details. The link leads

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			to a legitimate-looking website where you are asked to enter account and payment details. PayPal state on their website that they will NEVER ask customers for their password or credit card details via email. If you are required to take action in relation to your account, PayPal will use the secure message service within accounts to send you a message. Their website also has useful information about common PayPal scams and guidance on spotting genuine communications from the company. • **Ongoing Advice: Boiler Scam Calls -** West Dunbartonshire Council have warned that several local residents have received cold calls offering new boilers, where the caller claims to be working for the Council. The Council has confirmed that they will not contact people in this way and that they will send letters to tenants if they are going to be working in their area. As we reported last week, one of the most common phone scams in Scotland from April-June involved consumers being told that they needed to renew their boiler cover when their existing cover was in fact up to date. • **Nurseries/Early Years Providers -** The Competition and Markets Authority (CMA) has published an open letter and advice to nurseries and childcare providers to help them understand how consumer law applies to the arrangements they make with parents during the COVID-19 pandemic. They advise that, where businesses and parents have agreed to revise contracts, parents should not feel pressured into accepting new terms. If you have experienced an issue with a nursery or early years provider during the pandemic, you should contact Advice Direct Scotland in the first instance, either via their helpline on 0808 164 6000 or through their website.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			• **Ongoing Advice: HMRC Phone Scam -** We regularly report on various HMRC scams, texts and emails. This week, an elderly woman in the West of Scotland was cold called and told that she owed hundreds of pounds in tax. The woman said that her daughter dealt with her money and the caller then told the woman that if she told her daughter about the call, her daughter would go to prison. Thankfully the woman hung up, but was shaken by the call. Please make sure that elderly and vulnerable relatives are aware of these types of scams - find out more about avoiding HMRC scams and avoiding council tax scams on our website. **For more information and What to Do view Scam Share - Bulletin 20**
30 Jul 20	**Scottish Government Cyber Resilience Unit -** Sharing important information and guidance on COVID-19 related scams.	Cyber Resilience Notice - 30 Jul 2020	This Notice highlights: • **National Cyber Security Centre (NCSC) -** NCSC produce weekly threat reports drawn from recent open source reporting. View this week's report here. The NCSC has guidance how to defend your organisation against malware and ransomware attacks, including steps to take if your organisation is already infected. Police Scotland's Cybercrime Prevention Unit have created a handy guide to help your organisation protect your system from a Ransomware attack **Trending Topics:** • **Blackbaud -** In May of 2020, US based company Blackbaud, discovered and stopped a ransomware attack. Blackbaud is one of the world's largest providers of education administration, fundraising, and financial management software. At least 10 universities and over 125 charity organisations have been impacted as a result of this attack. Organisations impacted are now reaching out to their

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			stakeholders to inform them of a potential data breach, in line with Data Protection regulations. A statement on their website confirms that they 'paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed.' Although paying the ransom is not illegal, it goes against the advice of numerous law enforcement agencies, including the FBI, National Crime Agency and Europol, as there is no guarantee that you will get access to your device (or data). • **Garmin Fitness Tracker -** Garmin fitness devices have been left disconnected for nearly a day after the company suffered a major outage, possibly caused by a ransomware attack. Customers were not able to log into Garmin Connect to record and analyse their health and fitness data. This outage also affected their call centres and were unable to receive any calls, emails or online chats. Garmin has not officially confirmed the cause of this cyber-attack and has released an official statement about their recent outage. • **No More Ransom -** No More Ransom is an initiative by Europol's European Cybercrime Centre, is celebrating its fourth anniversary this month. The decryption tool repository site is designed to help define the type of ransomware affecting your device and check whether a decryption solution is available. Since its launch in July 2016,over 4.2 million visitors from 188 countries and has stopped an estimated $632 million in ransom demands from ending up in criminals' pockets. You should take precautions before running unknown tools on your devices. • **Rise in telephone scams as call centres reopen -** National Trading Standards is predicting a rise in scam telephone calls as illegitimate call centres around the world get back to work. One company was found to have made more than

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			680,000 automated scam calls over a four-week period, urging people to purchase face masks and hand sanitisers at a cost of £29.99 to £49.99 by falsely claiming that the PPE was a government requirement. Another common scam is victims receiving an automatic phone call, which claims that they've just been charged for an Amazon Prime subscription. The recipient is told that fraudsters have used their details to subscribe to Amazon Prime and that they can cancel the transaction by simply pressing 1. One variation of the scam claims that doing so will provide the recipient with more information, whilst a slightly different call promises to connect victims with an 'account manager' - who is in fact a fraudster. • **Fake Government helpline -** The Crown Prosecution Service has warned the public to beware of fraudsters exploiting the COVID-19 pandemic after a man was today jailed for 30 weeks for offering fake Government refunds. He obtained 191 sets of personal details and used 49 for fraud. The total loss to his victims was £10,019.17. One text message read: *'UKGOV: You are eligible for a Tax Refund as a result of the COVID-19 pandemic. Please fill out the following form so that we can process your refund'.* **For more information and what to do to reduce the risk view Cyber Resilience Notice - 30 Jul 2020**
23 Jul 20	**Trading Standards Scotland** latest scams across Scotland	Scam Share - Bulletin 19	This Bulletin highlights: • **Ongoing Advice: Travel Compensation Scams -** Fraud prevention service CIFAS are warning travellers to be wary of fraudsters posing as staff from travel companies, tour operators or insurers and offering to refund or rebook cancelled holidays. Scammers are also setting up fake websites offering refunds and compensation to holidaymakers. This follows warnings of fake caravan listings,

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			refund offers and travel deals from banking industry body UK Finance earlier this month. • **Ongoing Advice: Doorstep Scams -** This week, rogue traders have been targeting elderly and vulnerable people in the Central Belt. In one case, a scammer offered to replace the stones in an elderly consumer's driveway at a cost of £200. The scammer simply moved stones from the back garden to the front of the house. Another woman in the same area was charged £100 to trim a tree in her garden. Rogue traders have also been knocking on doors and charging £300 to pressure wash and seal driveways. They are willing to drop the price as long as consumers will pay in cash on the spot. • **Netflix Email Scam -** We have seen a new scam email saying that you can win a year's premium subscription to Netflix. Clicking on the link leads to a genuine-looking login page which is designed to steal your account and payment details. • **Pop-up Energy Adverts -** Since warning about misleading energy marketing scams linked to the UK Government's 'Green Homes' grant scheme, we have seen several examples of pop-up adverts on social media which imply that funding or grants for energy saving products are available to Scottish consumers. One example says that all Scottish homeowners are eligible for over £2,000 of funding and asks you to enter your personal details in order to apply. These adverts are designed to collect data and generate leads for companies who engage in misleading marketing. Clicking on these adverts leads to a form where you are asked to fill in personal details in order to determine whether you qualify for a grant. We are aware of Scottish consumers who have responded to these adverts and have then been called and visited by companies who pressured them into

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			signing expensive contracts for energy saving products that they did not want or need. • **Top 10 Scottish Phone Scams -** Scottish consumers continue to be hassled by a variety of nuisance calls. The most commonly reported phone scams in Scotland between April-June 2020 were: 1. Misleading sales of insurance for white goods, appliances or SKY equipment 2. Misleading sales of boiler, plumbing or drainage cover 3. Offers to reduce nuisance calls for a fee by signing you up to the Telephone Preference Service 4. Bank fraud - e.g. recorded messages saying that there has been a potential fraudulent transaction on your account and asking you to press 1 to discuss with an advisor 5. Attempts to gain remote access to your computer 6. HMRC frauds - e.g. saying that HMRC are filing a lawsuit against you and asking you to press 1 7. Amazon Prime scams 8. Claims management calls - e.g. offering services in relation to claiming backdated Marriage Tax Allowance or claiming tax owed on recent PPI payments 9. Misleading calls related to Green Deal funding 10. Offers of 'free' lottery tickets or calls advising that you have won a competition and asking for personal and bank details • **Bank Email Scam -** A recipient of Neighbourhood Watch Scotland Alerts has this week reported a scam email purportedly from the 'National Crime Investigation Centre' in the USA. The email addresses them as a 'scam victim' and says that

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			there has been an investigation into their bank, who may have delayed a payment in order to divert funds to another account. The recipient is advised to contact an officer using a Gmail account in order to receive a compensation payment. • **Local Listings: Business Scam -** Aberdeen City Council this week received a report of a scam targeting local businesses. Businesses were cold called and then received a follow up email with a seemingly simple request for them to confirm their address for local listings. However, the terms and conditions actually stated that the business would be liable for monthly payments if they responded to the email and signed the form. Businesses should be wary of similar scams and should ensure that anything they agree to sign not only comes from a trusted source, but that the details/terms are fully understood before they commit. A Scottish car dealer was also recently targeted by a scammer who applied for a UK Government Bounce Back Loan in their name and then tried to pay for a car using the funds. **For more information and What to Do view** Scam Share - Bulletin 19
22 Jul 20	**Police Scotland** Video Communications Platforms		Cyber criminals are trying to scam users of video communications platforms by sending out Phishing emails and Smishing texts, claiming to be from a video communications platform provider. These message formats claim to inform the recipient that they have a voicemail with relevant information about their account and to reply on an associated telephone number to retrieve the voicemail and alleged account information. What the recipient is not aware of is that the voicemail number is a premium rate number costing "£6 plus std net rate". Another Phishing email pretends to be a conference call invitation asking the recipient to click a link to "review invitation" to a meeting. Once the recipient has clicked on the link, they are unwittingly taken by the scammer to a Fake manufactured but genuine

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			looking login page which invites the recipient to upload their username and password. As they populate and submit their details, they are actually sending their personal login information directly to the scammers. Login information asked for to verify your details can include your customer account number, date of birth, email account details – very personal information to you and of value to a Scammer. Scammers use a range of scaremongering tactics to pressure people into clicking on links in Phishing emails or in response to Smishing texts. If you receive any suspicious or unsolicited emails or texts, please don't click on any links within them or reply to them. Instead make your own independent enquiry with your service provider and not using the unsolicited email or text as means to contact. You can report suspicious emails to the Suspicious Email Reporting Service (SERS): report@phishing.gov.uk and Spam texts to 7726.
16 Jul 20	**Trading Standards Scotland** latest scams across Scotland.	Scam Share - Bulletin 18	This Bulletin highlights: • **Ticketing Scams -** As more hospitality and event venues in Scotland are set to open over the next few weeks, demand for limited tickets and reservations could be high. Scammers may take advantage of this by advertising tickets which do not exist. If you receive an unsolicited email or see an advert on social media offering low prices on high-demand tickets, be wary. Always check the official website before purchasing a ticket that looks too good to be true. • **Visa Phone scam -** One of the most frequently reported phone scams in Scotland recently has been an automated call purportedly from Visa. The caller says that a £300 payment has been made to a Chinese charity from your account and asks you to press 1 to discuss blocking the transaction. Do not press 1 or follow any other instructions given in an automated message.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			• **DVLA Scam -** This week, consumer body Which? has reported a worrying new DVLA scam which targets those who have just renewed their vehicle tax online. The email says that your recent payment has failed and asks you to click on a link to verify your payment and contact details. The email says that, if you fail to update your billing details, you could be fined up to £1,000. In this case, the email address was from a German domain name and was clearly not linked to the DVLA (genuine emails will end in gov.uk). Scottish consumers have previously reported receiving other DVLA scam emails which say that their vehicle tax has expired and asks them to click on a link to make an immediate payment. The DVLA will not email and ask you to confirm your payment or personal details via a link. • **COVID-19 Crisis Grant Scam Text -** South Lanarkshire Council and Highland Council have this week reported a scam text message saying that 'crisis grants of £1,500 are available for individuals who need support during the Covid-19 pandemic'. The recipient is asked to click on a link for 'gov.crisis-grant.com'. HMRC has not sent any text messages about grants and links in any genuine messages from them will lead to the 'www.gov.uk' website. If you receive a similar text or email, do not click on any links. • **Ongoing Advice: Illegal Puppy Trade -** The SSPCA have published a new survey which shows that, despite increased demand for dogs during lockdown, over 80% of Scots think it is unsafe to buy a puppy online. 35% of respondents said that they were not confident that they could tell the difference between a genuine dog breeder and a puppy dealer. If you are considering buying a new four-legged friend, do plenty of research into the seller. Is their phone number or email address linked to different profiles? Are they advertising several different

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			breeds of dog? Are they reluctant to answer questions about the puppies' mother or provide paperwork? These are all signs that they may be involved in illegal puppy farming – find out more about spotting the signs on the SSPCA's Buy a Puppy Safely website. • **Boiler / Drainage Cover Scam -** One of the most frequently received scam calls in Scotland last month was offering boiler or drainage cover. In some cases the caller claims to be from a boiler servicing company and says that your boiler cover is due for renewal. They may ask for personal details or for a payment to renew your cover. If you receive a similar cold call and are not sure whether it is legitimate, hang up and contact the original boiler supplier to check whether you need to renew your cover. Do not give any personal details to a cold caller and don't agree to make any payments without confirming that the call is genuine. **For more information and What to Do view Scam Share - Bulletin 18**
16 Jul 20	**Scottish Government Cyber Resilience Unit -** Sharing important information and guidance on COVID-19 related scams.	Cyber Resilience Notice - 16 Jul 2020	This Notice highlights: • **Scammers continue to exploit COVID-19 -** Scams centred on exploiting COVID-19 have become prevalent in recent months. Everything from government grants and furlough payments, to mortgage holidays and demands for payment of fines, are being targeted by scammers utilising ever more sophisticated methods. Many scammers are using "phishing" and "smishing" (the term for phishing by SMS/text message) techniques to obtain sensitive information such as usernames, passwords and credit card details. They do this by disguising themselves as a trustworthy organisation in an email or text message, then by offering refunds or demanding payments, then direct the recipients to enter personal information on a fake website which matches the look and feel of the legitimate site. Always

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			question unsolicited requests for your personal or financial information in case it's a scam. Never automatically click on a link in an unexpected email or text message, and never immediately make a payment. Use trusted contact information to make enquiries with the organisation that the communication appears to be from - and do not reply to the initial email or text message. • **Ongoing Advice: Fake HMRC emails -** There have been reports of fake HMRC emails saying that your recent Coronavirus Job Retention Scheme application has been rejected or recalled and asking you to open an attached document. If you have received a similar email, don't download any attachments or click on any links. You can view HMRC Guidance on recognising scams if you're not sure. • **Updated guidance from Information Commissioner's Office (ICO) on holding data for Test and Protect -** With lockdown easing and hospitality venues re-opening, there is a requirement within the Test and Protect programme for places we visit to collect our personal data, to assist in tracing should there be an outbreak of the virus. The Information Commissioner's Office (ICO) has updated its Data Protection and Coronavirus Information Hub with guidance for people who are concerned about what their personal information is being used for, including what you should expect to be collected by staff at a venue you visit, how it should be stored and for how long it should be retained. Further information on this is available on the ICO Data Protection and Coronavirus Information Hub and within Scottish Government guidance for the hospitality sector on collecting contact details. • **Bounce Back Loan Scam -** Bounce Back Loans are a government scheme to assist genuine businesses through COVID-19 but the scheme has also been a

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			target for criminals. Not only are the lenders being targeted for fraudulent applications, but businesses are also being targeted and phished for their business data to be used in fraudulent Bounce Back Loan applications. Information on the Bounce Back Loan scheme can be found on the UK Government website. • **TECHNICAL GUIDANCE: Windows DNS Server Vulnerability: CVE-2020-1350 (aka SigRed) -** As part of the July 2020 security updates Microsoft have included an update for a critical remote code execution (RCE) vulnerability in Windows DNS Server. This vulnerability is 'wormable' and can be exploited by an unauthenticated attacker remotely over a network without any user interaction. Currently there are no known exploits for the vulnerability. Malicious actors and security researchers will be in the process of reverse engineering the updates and an exploit code will likely be released soon. Further information can be found in a Microsoft blog post. • **Bitcoin Investment Scams -** There have been reports of a number of US-based Twitter accounts being compromised on 15 July, and used to promote a scam enticing people to "send $1,000 worth of bitcoin and receive $2,000 back". Whilst the use of high profile accounts is new, double-your-money scams have been happening for years. If something seems too good to be true, it probably is. **For more information and what to do to reduce the risk view Cyber Resilience Notice - 16 Jul 2020**
10 Jul 20	**Police Scotland** Stop It Now! Scotland is a child protection charity	https://www.stopitnow.org.uk/stop-it-now-scotland/	Stop It Now Scotland provide confidential support services to individuals and families to protect the next child from harm and help prevent child sexual abuse. To enhance this work, Stop It Now Scotland have created an Upstream Prevention pack using the knowledge and experience they have gained over the past 12 years of working to keep

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
	dedicated to preventing child sexual abuse.		children safe from harm. These free resources are designed to be distributed to all audiences and across multiple platforms. The pack contains practical advice for professionals, individuals and families. If you wish to receive printed copies of any of these items, please get in touch with the team via scotland@stopitnow.org.uk. If you have been a victim of crime, and it is not an ongoing emergency, you can report this to Police Scotland on 101.
09 Jul 20	**Trading Standards Scotland** latest scams across Scotland.	Scam Share - Bulletin 17	This Bulletin highlights: • **Misleading Energy Marketing -** Following the announcement this week of the UK Government's new £2bn grant scheme to help homeowners in England with energy-saving home improvements, Scottish consumers should remain wary of misleading energy marketing scams. Uncertainty about the availability of energy efficiency incentives make it easy for dishonest companies to scam consumers. They say that funding or grants are available for their products, yet ask consumers to pay for the products up front or take out a loan. Consumers are told that they will receive their money back over time but rarely do. They often overinflate their prices and then apply 'discounts' which are supposedly equivalent to government grants. • **Prize Draw / Competition Scams -** The following scams have been reported in the last week: ➢ Fake emails purportedly from **Morrisons**, with the heading 'You Are Our Winner'. The recipient is asked to click on a link to discover what they have won. The link leads to a page saying that you have won a new iPhone - you are asked to enter your card details in order to pay a £1 'handling charge'. ➢ Consumer body Which? has warned about a fake **Currys/PC World** page on

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			social media which was offering free televisions if you liked and shared the page. These fake pages use 'offers' like this to build a following which could potentially allow them to attempt further scams on a larger audience. ➢ Fake **Primark** emails saying that you have been selected to participate in an anonymous survey about your experiences with the store and that you will receive 'exclusive reward offers' including vouchers if you complete the survey. ➢ Fake emails from **Aldi** thanking you for your loyalty and offering you an opportunity to win a £200 gift voucher. You are asked to click on a link to get started. • **Ongoing Advice: Scam Websites -** We have previously featured several stories about fake online stores, which have become more common during the lockdown period as more consumers have to purchase products online. This week, two Scottish consumers have complained about a website selling hot tubs which have not been delivered. One consumer discovered that there were a number of fake reviews for the company on Trust Pilot and that the official address listed on their website actually belonged to an empty shop. When shopping online, carry out some research before purchasing from sellers or companies you are not familiar with. Rather than relying on reviews hosted on the website you are purchasing from, look for independent reviews on official websites - try to check reviews on at least three different sites. When buying goods or services online, pay by credit card if possible, rather than bank transfer. This will offer you more protection if you are a victim of fraud. • **Ongoing Advice: Zoom Scams -** Staff working from home continue to be targeted by scammers. This week, the Chartered Trading Standards Institute has reported new email and text scams targeting home workers who use Zoom for

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. One text message, supposedly from 'Zoom Mail' says that the recipient has been sent a Zoom voicemail and that, to hear it, they should call a premium rate number that costs £6 plus the standard network rate. • **COVID-19 Job Retention Scam Email -** A recipient of Neighbourhood Watch Scotland Alerts recently received a scam email purporting to be from 'HMRC Business Help and Support'. The email said that 'your recent Coronavirus Job Retention Scheme application has been rejected or recalled' and had a spreadsheet attached, supposedly detailing contact information for a case officer. If you receive a similar email, do not download any attachments or click on any links. If you are not sure whether an HMRC email is genuine, check their website where they regularly update their list of genuine communications to help you avoid scams. • **Ongoing Advice: Amazon Scams -** Following our report in last week's bulletin about new Amazon Prime phone scams, more scams have been reported this week by Scottish consumers: ➢ A cold call claiming to be from Amazon's fraud department saying that the consumer's account had been hacked. The caller said that an iPhone had been ordered and asked for the consumer's mobile account details in order to secure a refund. The consumer provided the details and, after checking the transfer details, discovered that the money had gone to an account based in Africa. They are still receiving cold calls from the same number. ➢ Automated calls saying that the consumer will be billed £59.99 for Amazon Prime and that they should press 1 to be put through to an account manager. • **Ongoing Advice: Face Masks -** From 10 July, wearing a face covering will be

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			compulsory (with certain exceptions) in shops in Scotland - it is already compulsory on public transport. Consumers should remain wary of masks or face coverings being sold through online marketplaces or from unknown sellers which claim to be PPE or to offer medical-grade protection. Counterfeit or poorly made masks may offer a false sense of security and may not provide the advertised level of protection. • **Training Scams -** The SBRC have reported a new scam targeting employees returning to offices, which was uncovered by Check Point Research. Many organisations have offered webinars or online training to explain new rules and procedures to staff returning to offices after lockdown; however, scammers are exploiting this by sending fake emails which appear to offer training materials. Some of these emails ask recipients to click on a link to register for a training session - they are taken to a fake website which asks them to enter their Microsoft login details. **For more information and What to Do view Scam Share - Bulletin 17**
08 JUL 20	**Police Scotland** ICT System Privileges and Access & Ransomware Attack	https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/managing-user-privileges https://www.ncsc.gov.uk/collection/passwords https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security	**ICT System Privileges and Access** Computer networks can be compromised in a variety of ways from direct cyber-attacks to phishing emails and these attacks reference a wide array of threats based on topical themes, such as those exploiting the current crisis to carry out fraudulent activity. Cyber-attacks can affect you or your business in a variety of ways, such as harm and impact on your reputation to the risk of losing data, all of which can be very difficult to recover from. As businesses and organisations slowly begin to return to work, they should take this time to consider their ICT policies and what they expect from their staff in terms of maintaining business security. Generally speaking, ICT systems that have

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
		Cyber Security Centre website: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks . Have you received a suspicious email? Forward it to the National Cyber Security Centre Suspicious Email Reporting Service (SERS): https://www.ncsc.gov.uk/information/report-suspicious-emails And the associated link reporting@phishing.gov.uk	been carefully designed can minimise most vulnerabilities however these efforts can easily be undone, e.g. If all your staff have ICT admin user privilege access, the vulnerability to your system security is increased. This risk can be managed by providing all users with the reasonable (but minimal) level of system privileges and rights required for their role, this principle is sometimes referred to as 'least privilege'. Businesses and organisations should consider having a policy in place where they allocate minimum system user access to general staff. Increased user system privileges should be allocated to qualified individuals being carefully reviewed, controlled and managed on a regular basis. By introducing these steps you support staff by raising awareness regarding Cyber security, acceptable account usage and their personal responsibility to adhere to corporate security policies. **"Your files are encrypted and currently unavailable"** What would you do if you logged into your computer network and instead of seeing all your files you saw this message? This is exactly what happened to a company when they discovered that their system had been infected with Ransomware and all their files were unavailable. No matter how many times the company employees restarted their networked computers all users were met with the same message. Ransomware is a type of malicious software which will stop you from accessing the files on your computer. Police Scotland's guidance to help your organisation protect your system from a Ransomware attack.
02 Jul 20	**Trading Standards Scotland** latest	Scam Share - Bulletin 16	This Bulletin highlights: • **Shut out Scammers -** During the nationwide Shut out Scammers campaign, run in partnership with Police Scotland from 15-26 June, a bogus trader was

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
	scams across Scotland.		sentenced to four years in prison after targeting elderly and vulnerable householders in Ayrshire. The scammer would knock on doors and claim to be a gardener or window cleaner, asking for money for services or repairs which were never completed. • **Holiday Scams** - Amidst continuing uncertainty about travel restrictions, banking industry body UK Finance has warned consumers to be wary of holiday scams, including fake caravan listings, refund offers and travel deals. Some of the scams to be aware of include: ➢ Fake listings for caravans/motorhomes at low prices on social media or auction sites. Potential buyers are told that they can't view the caravan in person due to lockdown restrictions - the vehicle often doesn't exist or isn't delivered; ➢ Scam calls, emails or fake posts on social media advertising holiday refunds. You may be asked to pay an upfront fee as payment for handling a refund claim; ➢ Fake websites advertising cheap holiday deals. These can look similar to genuine websites, with similar URLs and ask for deposits for holidays which often don't exist. • **Amazon Phone Scam -** Police Scotland have recently received several reports from consumers who have had cold calls purportedly from Amazon Prime. In some cases, they are told that their subscription is due for renewal and that an automatic payment will be deducted from their bank account. Other calls say that a button has been clicked and that a payment is due as a result, but that the caller can help them secure a refund. In both cases, the caller, who appears to be phoning from within Scotland, asked consumers to visit a website and download

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			either software or an app in order to check their account. Downloading this software will grant the scammer access to your computer. • **BT Phone Scam -** Several Scottish consumers have recently received cold calls purportedly from BT saying that their line is going to be disconnected due to suspicious activity in their area and asking them to press 1 to speak to an advisor. One consumer pressed 1 and was connected to someone in an overseas call centre. Thankfully, they realised that it was a scam and immediately hung up. Another consumer received an automated call saying that their BT bill was going to be increased and asking them to phone a number provided to discuss their account. The consumer was not with BT, so immediately ended the call. • **British Gas Scam -** Action Fraud have received over 2,500 complaints about scam British Gas emails, which lead to fake websites designed to harvest your personal and financial information. The emails say that your gas service will be cut off if you don't pay an outstanding bill and ask you to click on a link to make a payment. • **Pension Scams -** As research from the All-Party Parliamentary Group on Pension Scams has found that it is increasingly likely that pension savers will be contacted by scammers via phone or online while at home during the Covid-19 pandemic, the work and pensions committee has this week been called on to open a formal inquiry into pension scams. The Association of British Insurers (ABI) advises consumers not to respond to unsolicited calls, emails or texts about pension reviews and to check that a provider is authorised by the FCA before dealing with them. • **Life Insurance & Banking Scams -** Scottish consumers have recently received

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			cold calls saying that they are due to receive a sizeable life insurance refund. They are asked to provide personal and financial details in order to process the payment. Age Scotland have also warned about banking scams after a man in his 80s from East Dunbartonshire almost fell victim to a sophisticated phone scam last month. He received a call from his bank's phone number, which had been cloned by scammers, and was told that there had been fraudulent transactions on his account. He was asked to transfer money to a new account and was given a new number and sort code. Thankfully, he was suspicious and contacted his bank independently - they verified that the original call had been a scam. • **Ongoing Advice: HMRC Scam -** We recently featured an HMRC scam targeting self-employed workers using the Self-Employment Income Support Scheme. The text says that the recipient is eligible for a tax refund under the scheme and asks them to click a link which leads to a fake HMRC website where they are asked for personal and financial details. • **Ongoing Advice: Business Scams -** A recent study by IBM has shown that almost half of those working from home during the Covid-19 pandemic are concerned about cybersecurity risks. Companies across the UK continue to be targeted by scammers sending fraudulent emails requesting information and financial details related to COVID-19 Retail, Hospitality and Leisure grants. The emails claim to be from clients or employees of the business and may ask for account or business rate reference numbers for retail outlets. **For more information and What to Do view Scam Share - Bulletin 16**
02 Jul 20	**Scottish Government**	Cyber Resilience Notice - 02 Jul 2020	**WhatsApp** An alert has been issued about a 'sophisticated' WhatsApp scam. Hackers have

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
	Cyber Resilience Unit - Sharing important information and guidance on COVID-19 related scams.		targeted thousands of profiles, telling users that their accounts need to be verified. The new version of the scam comes from a user named the "WhatsApp Technical Team". The profile picture feature the WhatsApp logo - and the account asks users to verify their identity by sending over their six-digit log-in code. In another example, the criminals will pose as a friend, saying they have accidentally sent their authorisation code over to you. This is a trick to get your own login code, which in turn will give hackers access to your account, so they can send a text to your contacts and read all of your messages. WhatsApp never asks for your data or verification codes. To stay safe, set up two-factor authentication on your accounts, with controls usually found within your account settings. That means that even if someone gets access to your six-digit number they will still need an extra password, which adds an extra layer of security for your private details. **For more information and what to do to reduce the risk view Cyber Resilience Notice - 02 Jul 2020.**
25 Jun 20	**Trading Standards Scotland** latest scams across Scotland.	Scam Share - Bulletin 15	This Bulletin highlights: • **Phone Scams -** As Trading Standards launch the rollout of call blocking devices, some of the phone scams most commonly reported by Scottish consumers are: ➢ Cold calls trying to sell you insurance or a new warranty for various appliances, including white goods, televisions and solar panels ➢ Various calls purportedly from HMRC saying that you have committed tax fraud and that a warrant has been issued for your arrest or that you are due a tax rebate and asking you for personal and bank details ➢ Cold calls purportedly from Microsoft or your broadband provider asking for remote access to your computer or saying that your service will be cut off unless you pay a fee

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			➢ Automated calls purportedly from your bank saying that a payment has been sent overseas from your account - you are asked to press 1 to speak to an advisor ➢ Cold calls carrying out a health survey or offering to arrange a home visit to sell mobility aids ➢ Misleading energy marketing calls advertising grants for energy saving devices, trying to sell warranties for solar panels or carrying out surveys about double glazing • **Football Streaming -** With millions of football fans across the country expected to log in to streaming services to view matches being played behind closed doors, the National Cyber Security Centre is warning fans to be careful to secure their accounts and devices. They have published advice on choosing strong passwords and keeping streaming apps updated on their website. Stay safe when buying streaming or other electrical devices online - use the Vistalworks checker to make sure that products purchased online are genuine and read more about the dangers of using illegal streaming services and devices in their blog. Get advice on staying safe while gaming and streaming online from the National Cyber Security Centre and Get Safe Online. • **Online Surveys -** A Scottish consumer was sent a survey this week on social media saying that if they shared the link, they would have a chance of winning a house. When they clicked on the link, they were taken to a form which asked them to input their details, including bank details and security code. We have previously featured similar scams in the bulletin, where consumers are asked to fill in surveys on social media to win chocolate or shopping vouchers.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			• **National Insurance Scam -** Some of our colleagues have received scam emails this week purporting to be from the UK Government, saying that they have established a 'new tax refund programme for dealing with the coronavirus pandemic'. The official-looking email (with Government logos) goes on to say that, based on your National Insurance contributions, you are eligible for a tax refund. You are asked to click on a link to access your refund. • **Ongoing Advice: Face Masks -** With face masks now mandatory on public transport in Scotland, consumers should remain wary of masks or face coverings being sold through online marketplaces or from unknown sellers which claim to be PPE or to offer medical-grade protection. Counterfeit or poorly made masks may offer a false sense of security and may not provide the advertised level of protection. • **Price Gouging -** With more retail outlets due to open in the next few weeks, the CTSI, the CMA and other organisations have called for a stop to unscrupulous price gouging. They are urging businesses not to engage in unfair pricing practices amid concern that price gouging will increase once shops open, particularly where products are in high demand. Since March, the CMA has written to 264 traders about unjustifiable price rises, following over 3,000 complaints from consumers. If you see a business behaving unfairly, you can use their online reporting tool. **For more information and What to Do view Scam Share - Bulletin 15**
25 Jun 20	**Scottish Government Cyber Resilience**	Cyber Resilience Notice - 25 Jun 2020	This Notice highlights: • **Text and Private Messages Scams -** The consumer rights organisation Which has drawn attention to a credible direct message pretending to be from

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
	Unit - Sharing important information and guidance on COVID-19 related scams.		Instagram's help centre. The message is sent to private inboxes on the photo-sharing app, and warns the user that one of their posts has infringed copyright law. It threatens to close the user's account within 24 hours. The message is a phishing scam, encouraging you to click on the link to dispute the claim and to disclose personal information. Instagram contacts its users about account information over email, so the advice is to delete the message if you receive one. Text scams supposedly coming from the phone companies like Three and O2 have been reported to Citizens Advice Scotland. Consumers noted that texts appear to have come from the phone company. The texts state that the recipient's latest bill has not been paid and that they need to verify their payment details via a link. The companies have a range of helpful advice on the Three and O2 websites to help users spot SMS phishing attempts. • **Fake COVID-19 home testing appointment texts targets public** - The Chartered Trading Standards Institute (CTSI) has witnessed evidence of bogus texts informing members of the public that a "COVID Home Testing Team" will soon visit their homes. The text specifies a date and time for the visit and that the "team" will telephone the recipient upon arrival. The text becomes suspicious where it states that the team "will enter your property and we will remain inside the front door to put on our protective clothing. You must wait in a separate room before we come to you." This is an attempt by thieves to gain access to people's homes under cover of COVID-19 measures. NHS Test and Trace will never ask you for financial details, PINs or passwords. They will also never visit your home. There is more information on NHS Scotland's Test and Trace in last week's bulletin and check out this video for advice on what to expect from a genuine contact tracer call.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			• **Call Blocking Devices -** As part of the #ShutOutScammers campaign, Trading Standards Scotland are launching the rollout of free call blocking devices to vulnerable Scottish consumers who are most at risk from scammers and rogue traders. The Scottish Government has provided £15,000 in match funding to Trading Standards Scotland to procure 280 trueCall call blocking devices which are available free of charge. Find out more information on the Trading Standards website. • **ThinkUKnow** - ThinkUKnow is an education programme from National Crime Agency (CEOP) which protects children both online and offline. They have created a range of guidance to support parents during COVID-19 and the closure of schools. Every fortnight, they aim to release a new presentation for parents and carers to help with online safety at home. Regrettably amongst our children and young people there is a common trend of sharing sexual imagery of themselves on messaging apps. This is a concerning issue which can put young people at risk of embarrassment, bullying and increased vulnerability to sexual exploitation. CEOP links to range of hot topics which cover internet safety advice on the dangers of sending nude pics, sexting and more to help provide support on these topics. A report published by Europol shines a light on the increased sharing of child sexual exploitation images online and how to confront this serious threat to children's safety. See useful presentation from Police Scotland. **For more information and what to do to reduce the risk view Cyber Resilience Notice - 25 Jun 2020.**
18 Jun 20	**Trading Standards**	Scam Share - Bulletin 14	This Bulletin highlights: • **Ongoing Advice: Doorstep Scam -** This week, one of our own colleagues was

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 latest scams across Scotland.		cold called by two females and a male in a liveried van who said that they had ordered a number of trees for a nearby building complex. They said that due to the COVID-19 pandemic, the houses were not yet ready and so they were selling the trees at a discounted rate. They offered the trees for £40 and £60. This is a frequently used tactic by doorstep scammers - they may offer to carry out work in your garden or lay a tarmacadam driveway at a discounted rate because they "have excess materials left over from another job which they need to use up". They try to pressure you into agreeing to allow them to start work immediately. • **Ongoing Advice: Contact Tracing Scams -** Scottish consumers are continuing to report contact tracing scams linked to NHS Scotland's Test and Protect service. East Dunbartonshire Police received reports this week about a phone scam where a cold caller claiming to be from the NHS told the consumer that they had been in contact with someone who tested positive for COVID-19. The caller tried to obtain bank details and payment for testing kits. Genuine contact tracers will NEVER ask you for any financial details or ask you to make a payment. They won't ask you to create a PIN number, ask for details of your social media accounts or ask you to download anything. • **Ongoing Advice: Online Shopping -** NatWest have reported a fivefold increase last month in the number of online scams where customers paid for items on fraudulent websites which were never delivered. We have featured reports of fake websites in several bulletins since lockdown began, as fraudsters use the lure of popular items which are sold out in official stores to scam consumers. This week, Which? have warned about fake adverts for Clarks shoes which have been popping up on social media. In some cases, consumers who had ordered and paid

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			for shoes were sent a scarf instead. • **Ongoing Advice: Tax Rebate Scam -** A consumer received an email this week purporting to be from 'Government Gateway'. The official-looking email (with Government logos) said that, as a precaution against COVID-19, the Government had established a new tax refund programme and that the recipient was eligible for a tax rebate of £519. The recipient was asked to click on a link to access their refund. In April alone, HMRC received over 43,000 complaints about phishing emails. They regularly update their list of genuine communications to help you avoid scams. Find out more about avoiding HMRC scams and avoiding council tax scams on our website. • **Working From Home -** When working from home, remain wary of unexpected emails which appear to be from a current or previous colleague. Our own staff have this week received emails supposedly from a former colleague, asking them to provide their phone number so that they can be updated on a pending task. The emails were sent from a suspicious-looking Gmail account which did not match the name of the supposed sender. • **Fake COVID-19 Testing Kits -** A man was arrested in London last week for allegedly selling over 500 fake coronavirus testing kits online. The National Crime Agency say that they are continuing to investigate the sale of various counterfeit products relating to COVID-19. The MHRA has confirmed that: "No COVID-19 antibody self-testing kits have received CE mark status and there are no such testing kits available in the UK for home use." • **HSE Email Scam -** A Scottish consumer reported a fake email from HSE to Neighbourhood Watch Scotland this week through their ALERT system. The email

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			advised that the consumer's business was being investigated for breaking guidelines and that the nominator would remain anonymous until the court hearing. A spreadsheet was attached, supposedly containing more details about the case. The consumer contacted HSE, who confirmed that the email was a scam. **For more information and What to Do view Scam Share - Bulletin 14.**
18 Jun 20	**Scottish Government Cyber Resilience Unit -** Sharing important information and guidance on COVID-19 related scams.	Cyber Resilience Notice - 18 Jun 2020	This Notice highlights: • **National Cyber Security Centre (NCSC) -** The National Cyber Security Centre recently produced guidance aimed at helping organisations that are moving their business online. This guidance will help you determine how ready your business is, and point the way to any new cyber security measures you should put in place. Having a good relationship with your IT service provider(s) will help with this. NCSC have identified and explained the key cyber security topics you should be concerned with, so you can be sure you're covering all bases. • **Football fans online streaming accounts and subscriptions -** Millions of football fans are expected to log into subscriptions to stream behind-closed-door games. NCSC warns online hackers could break into football fans' accounts to carry out 'phishing' scams. The NCSC has urged fans to take some basic steps, which form part of the NCSC's Cyber Aware behaviours, to keep their accounts secure, including setting strong passwords that are made up of three random words and ensuring you download the latest updates for apps on devices. **Trending Topics:** • **Black Lives Matter ransomware -** Hackers have been taking advantage of recent events and the popularity of the Black Lives Matter movement. There have been

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			reports of ransomware being spread through phishing emails, targeting those in areas where there have been Black Lives Matter protests. A typical email asks users to fill in a confidential survey to comment on the recent protests, then asks them to download an attachment to fill out a form. The form contains a piece of malware known as "TrickBot" which is a common ransomware program. This will encrypt a user's files and attempt to steal sensitive information such as banking details and passwords that may be saved on the computer/device. Since last Thursday, there has been increase in the number of new domain names registered containing words related to the campaign which may be used in phishing attempts. • **Donating to charities online -** Get Safe Online has valuable advice when donating to charities online. Take time to make you sure you are safe to proceed, by checking the web links and charities' official web pages for information. Be cautious of any links asking you to donate. Make sure to verify that your donations are going to a trusted organisation. In Scotland, all charities must be registered, and an online register of charities is maintained by the Office of the Scottish Charity Regulator (OSCR). • **Kids at home -** As a parent or someone else with responsibility for a child or young person, you'll be all too aware of the dangers they can be exposed to online. Get Safe Online safety experts have put together some expert tips to help you keep the children and young people in your care safe and more aware of these dangers. They also have some simple checklists to help you keep your kids safe online according to their age group. • **Cyber Resilience COVID-19 Bulletin Scams Awareness Fortnight 2020 -** Citizens Advice Scotland has welcomed the launch of their 2020 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**
			Awareness campaign which runs from 15-28 June. The 2020 campaign objective is to reduce the risk and impact of coronavirus scams by raising awareness and encouraging behaviour change amongst the public at a local and national level. For further information, visit Citizens Advice website Scams Awareness Fortnight 2020. (Please note that the material provided by Citizens Advice includes England-only contact information.) Alongside this campaign, the Advertising Standards Authority (ASA) in partnership with the Internet Advertising Bureau, launched a new scam ad alerting system. This allows internet users to report scam ads appearing in paid-for space online to the ASA. It will then send an alert to advertising platforms and publishers with details of the scam ad. You can report an ad using this form on the ASA website. Use this form to report online scam ads including ads on newspaper websites, paid-for search engine ads or ads appearing on social media. For more help on spotting scams and how to protect yourself online, Martin Lewis(money saving expert)has some great articles including: 30+ ways to stop scams and 20+ coronavirus scams to watch out for. Please note that if you wish to participate in the Scam Awareness campaign in Scotland, use the provided campaign materials, or reporting a scam ad online– please use and promote the links below. This will help to ensure Scottish consumers are directed to the most appropriate sources of information, advice and/or scams reporting helplines **For more information and what to do to reduce the risk view Cyber Resilience Notice - 18 Jun 2020**
11 Jun 20	**Trading Standards**	Scam Share - Bulletin 13	This Bulletin highlights: • **Ongoing Advice: Contact Tracing Scams -** Following our warning about contact tracing scams linked to NHS Scotland's Test and Protect service last week, there

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 latest scams across Scotland.		have been reports from Scottish consumers about cold callers who say that you have been in contact with someone who has tested positive for COVID-19 and ask you to pay £500 to take a test. Genuine contact tracers will NEVER ask you for any financial details or ask you to make a payment. Genuine contact tracers will give you a number that you can call to verify their identity. Some NHS boards have published contact numbers that people can phone to confirm that a contact tracing call is genuine. Where a specific contact number has not been published, you should contact the main switchboard of your local NHS board - find their contact details here. • **Ongoing Advice: Online Shopping -** There are ongoing problems with websites which are taking payments for orders but not delivering them and not communicating with consumers. In the last week, Scottish consumers have reported websites selling gardening equipment, bicycles and sportswear which have taken money from their account but failed to provide an order confirmation or to respond to emails or phone calls. In the cases reported, the consumers have carried out research online and have discovered that a number of other customers have complained about the same websites. Vistalworks have published a new article about shopping safely online. • **Ongoing Advice: Pension Scams -** The Pensions Regulator has repeated its warning about pension scams during the COVID-19 pandemic. A recent study showed that 1 in 5 victims of financial scams since the beginning of the outbreak had been targeted by pension scams, such as fraudsters offering a 'free' pension review. • **HMRC Scams -** A new HMRC scam targeting self-employed workers using the

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			Self-Employment Income Support Scheme has been reported this week. The text says that the recipient is eligible for a tax refund under the scheme and asks them to click a link which leads to a fake HMRC website where they are asked for personal and financial details. • **Streaming Scams -** The European Consumer Centre Network has published a 'Safer Streaming' report looking at the threats from using illegal video streaming services. There has been an increase in the number of scam streaming sites, which ask users for personal and financial details but do not then provide the streaming content advertised. • **Ongoing Advice**: **Cancellations & Refunds -** After the CMA announced that they would be investigating cancellations and refunds in the travel industry, a holiday lets company has changed their refund policy and has committed to offering all customers a full refund if their booking was cancelled due to the COVID-19 outbreak. • **Ongoing Advice: Face Masks -** The World Health Organisation is now recommending that people should wear fabric face coverings in situations where social distancing isn't possible and that the over-60s should wear medical masks in some circumstances. The Scottish Government advice is currently to wear a face covering in enclosed spaces where social distancing is more difficult. Online scammers may take advantage of an increase in demand for face masks and coverings to sell sub-standard products or to sell them at inflated prices. Be particularly wary of unfamiliar new websites selling PPE and of pop-up adverts on social media. • **Microsoft Scams -** People working from home have been targeted by scam

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			emails which appear to be from their IT department and ask them to click on a link to update their connection to the company network. When they click on the link, they are directed to a fake Office 356 login page where they are asked to enter their details. This allows the scammers to access their Office 365 account. • **Ongoing Advice: Illegal Puppy Farms -** A new Welfare of Dogs (Scotland) Bill has been introduced to the Scottish Parliament which proposes to improve the welfare of puppies and dogs by strengthening the system for licensing dog breeders and discouraging illegal puppy farming. There have been several online puppy scams reported by Scottish consumers in recent weeks as demand for puppies has risen sharply during the lockdown. • **Bank Transfers -** TSB have highlighted a case this week where a Scottish consumer purchased a bicycle on an online marketplace. The seller claimed that they were an NHS worker who was self-isolating and asked for the payment to be made via bank transfer - the consumer paid £200 but did not receive the bike. In this case, due to the bank's fraud refund guarantee, the consumer received a full refund. When buying goods or services online, pay by PayPal or credit card if possible, rather than bank transfer. This will offer you more protection if you are a victim of fraud. **For more information and What to Do view Scam Share - Bulletin 13.**
11 Jun 20	**Scottish Government Cyber Resilience Unit -** Sharing	Cyber Resilience Notice - 11 Jun 2020	This Notice highlights: • **National Cyber Security Centre (NCSC) -** NCSC produce weekly threat reports drawn from recent open source reporting. View this week's report here. **Trending Topics:**

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
	important information and guidance on COVID-19 related scams.		• **Fake COVID-19 testing kits** - A man in Birmingham has been arrested for allegedly selling 500 fake testing kits for COVID-19 on the dark and open web. The arrest is part of the National Crime Agency's response to criminals attempting to exploit the COVID-19 pandemic. • **Furlough, refund and grant fraud** - Scams centred on exploiting COVID-19 have become prevalent in recent months. Everything from Government grants, furlough payments, requests for refund of overpayments, to mortgage-holidays, are being targeted by scammers, using ever-more sophisticated methods. Many scammers use "phishing" to obtain sensitive information such as usernames, passwords and credit card details. They do this by disguising themselves as a trustworthy organisation in an email or text message, perhaps offering refunds or government grants. They often ask recipients to enter personal information into a fake website which matches the look and feel of the legitimate site. Always question unsolicited requests for personal or financial information in case it's a scam. Never automatically click on a link in an unexpected email or text message. If the email or text message tells you that you have been overpaid a grant or furlough payment, or contains a demand for payback, use trusted contact details for your employer or the relevant government department to find out if the request is genuine - and never immediately make a payment. • **HMRC bogus tax refunds -** HMRC has warned students to be alert to a fresh wave of cyber frauds aimed at them, offering bogus tax refunds. Last week saw a sudden spike in students reporting suspected scams received at their official university email addresses. Experience shows that when new scams emerge targeting students, they often multiply. We therefore want to warn students to take

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			a moment to think before parting with their personal information. ➢ Scam emails say that the student is owed a tax refund and invite them to click on a link to 'complete the required form'. They add: 'If you do not complete the refund form now, you will not be able to claim your tax refund online.' Criminals will then use the malicious link to harvest students' personal data. ➢ The emails include a scam warning, saying: 'If you're unsure an email is from HMRC do not reply to it or click on any links.' If you suspect you have received such an HMRC Scam email you can report this directly to HMRC using the email address: phishing@hmrc.gov.uk. HMRC guidance on phishing and scams is available at www.gov.uk/topic/dealing-with-hmrc/phishing-scams. • **Patching and updates: Largest ever Microsoft 'Patch Tuesday' and Zoom update advice -** On Tuesday 9 June, Microsoft issued their largest ever monthly 'patch Tuesday' update, which patches 129 vulnerabilities. Users of Zoom should update their version to the latest 5.0 release, which became available mid-May. This patch addresses many of the security issues previously highlighted in this popular video conferencing platform. Users who have not updated to the latest version are finding issues with access to virtual meeting calls. Organisations that host events using Zoom are asked to encourage their attendees to ensure they have the correct version at the point of sign up. NCSC guidance on installing the latest software and app updates is available here. • **Scam third party sellers on Amazon -** Back in February, Amazon banned more than one million product listings related to COVID-19 from third party sellers, where listings were seen to be "price gouging" or selling fake products with misleading health claims. Huffington Post recently revealed that some products

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			may still be slipping through, including counterfeit medical supplies, hand sanitiser, UV lights, supplements and non-expert books on COVID-19. Consumers who haven't received goods or who have received goods in an unsatisfactory condition can request a refund from the seller and may be eligible for an Amazon 'A-to-Z Guarantee' refund. • **Doctor scam** - Doctor surgeries have highlighted that some of their patients have been contacted by a bogus doctor. The patients have been asked for their bank details to pay for a prescription under the COVID-19 regulations. This is a scam and you should never give your bank details to someone claiming to be your doctor. If you have been affected, please contact your bank card provider and report this to Police Scotland on 101. **For more information and what to do to reduce the risk view Cyber Resilience Notice - 11 Jun 2020**
04 Jun 20	**City of London Police National Fraud Intelligence Bureau** Coronavirus fraud core script		**Government smishing** The Government has only sent one text message to the public regarding new rules about staying at home to prevent the spread of COVID-19. Any others claiming to be from UK Government are false. Criminals are able to use spoofing technology to send texts and emails impersonating organisations that you know and trust. If you receive an unexpected text or email, asking for personal or financial details, do not respond. Remember, don't click on the links or attachments in any texts or emails and instead visit the official website through a known route. The public can report any type of SMS scams by forwarding the original message to 7726, which spells SPAM on your keypad. **What scams are we seeing?**

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			• **Vehicle for sale online -** Suspect advertises a vehicle for sale online but says it can't be viewed in person, due to the lockdown restrictions. The suspect instead arranges for the vehicle to be delivered using a delivery company. The victim pays for the vehicle (or a deposit), but the vehicle is never delivered. The victim is given the option of paying by bank transfer or through PayPal. The PayPal link they're provided with is a spoofed site. • **Wall mounted hand gel dispensers -** The highest loss reported in the last 24 hours was for £41,616, which related to a bulk order for wall mounted hand gel dispensers which never arrived. These dispensers were ultimately supposed to be for the NHS. • **Dating fraud -** A dating fraud in which the suspect claimed to have contracted the coronavirus and needed help with medical bills • **Furlough scheme -** A suspect used the government's furlough scheme to claim for an individual who doesn't work for them. **International cash grants and relief funds** There has been a new phishing attempt reported, claiming to be from the World Health Organisation (WHO), offering cash intervention grants to selected individuals for the sum of $950,000 as a result of the outbreak. This is a similar modus operandi to what has been reported before, although there have been some minor changes to the messaging content and the contact email address used by the criminals to deceive recipients. Recipients are told they will receive their funds through an ATM card insurance and are asked to contact the sender via email (manager@swisscard.org) for more information on how to receive these funds. They are told they need to respond

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			within 10 days to ensure they receive these payments. Another new but similar type of phishing attempt has emerged, purporting to be from the IMF Global Pandemic Relief Fund, informing recipients that they have been awarded a sum of $650,000mil dollars by the fund as a result of the outbreak. Recipients are asked to contact the bursary official to request for further details on how to receive the money.
04 Jun 20	**Trading Standards Scotland** latest scams across Scotland.	Scam Share - Bulletin 12	This Bulletin highlights: • **Community Signposts -** As communities deal with uncertainty and isolation during the COVID-19 outbreak, there are many who require help from others and many who wish to volunteer their time and services. Find out more about Scotland's voluntary sector from SCVO. During Volunteer Week Scotland, we have developed 'Community Signpost' guidelines in relation to doorstep scams and community safety, both for those who want to help others in their community and for those who require assistance: ➢ Stop uninvited callers on your doorstep ➢ Check who you are dealing with ➢ Wait to make a payment ➢ Avoid cyber and phone scams ➢ Report suspicious callers or activities • **Freshers Week Scams -** There have been warnings about scammers targeting young people preparing to start at universities in September. With many student unions still to confirm Freshers Week events due to uncertainty about the lockdown, the National Union of Students (NUS) is warning young people to be

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			wary about buying tickets for events online. Fraudsters are creating fake events which appear to have been organised by student unions and selling tickets to unsuspecting students. • **Contact Tracing Scams -** Throughout the COVID-19 pandemic, scammers have been keeping up to date with the latest developments. Now, with the launch of the Scottish Government's Test and Protect service last week, consumers are being warned to be wary of fraudsters posing as contact tracers. There have been reports from around the world of contact tracing scams, including fake texts highlighted by the CTSI in May. These texts say that you have come into contact with someone who has tested positive or has shown symptoms for COVID-19. You are asked to click on a link to find out more information - this link leads to a fake website which will ask for your personal or bank information. • **Scams Related to 5G Conspiracies -** Amidst widespread 5G conspiracy theories, Trading Standards officers have examined a USB stick being marketed as a '5G BioShield' offering a 'wearable holographic nano-layer catalyser'. The device, which was being sold for over £300, was in fact no different to any other USB stick with 128mb of storage. • **Bitcoin Scams -** A crypto intelligence company has said that there are increasing numbers of scams related to COVID-19 which require payment in cryptocurrency. £1.4 billion has already been lost in cryptocurrency fraud this year. In some cases, scammers have posed as Red Cross workers and asked for donations in cryptocurrencies, while others have sold fake PPE, treatments or testing kits. • **Travel Cancellations: Quarantine -** There is likely to be some confusion around travel cancellation and refund rights as the new quarantine rules are enforced. If

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			you have been affected by any travel/accommodation cancellations and are unsure about your consumer rights, contact Advice Direct Scotland on 0808 164 6000 or visit their website. • **PPE and Face Masks -** The Office for Product Safety and Standards has updated their guidance for manufacturers and makers of face coverings. Anyone selling face coverings must ensure that they meet the existing requirements of the General Product Safety Regulations 2005. It was reported this week that 6.5 million sub-standard face masks and 8,000 counterfeit hand sanitisers have been seized by Trading Standards officers at Heathrow Airport since the start of the COVID-19 pandemic. According to the Journal of Trading Standard, many of the masks seized either had fake safety certificates or made false claims about their effectiveness - others did not meet UK safety standards. The hand sanitisers seized had fake labelling and packaging, which was identical to those of genuine brands. Trading Standards officers have found several other instances of retailers selling counterfeit hand sanitisers, some of which contained dangerous ingredients. • **Counterfeit Toys -** This is Child Safety Week and consumers are being reminded to be wary of counterfeit toys being sold online which won't have gone through quality testing and might contain dangerous materials, loose parts and sharp edges. It can be tempting to buy an in-demand toy which is advertised at a knock-down price on ebay or other online marketplaces; however, cheap fakes often do not meet UK health and safety standards. **For more information and What to Do view Scam Share - Bulletin 12**

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
04 Jun 20	**Scottish Government Cyber Resilience Unit -** Sharing important information and guidance on COVID-19 related scams.	Cyber Resilience Notice - 04 Jun 2020	This Notice highlights: • **National Cyber Security Centre (NCSC) -** NCSC produce weekly threat reports drawn from recent open source reporting. View this week's report here. • **Scotland's Serious Organised Crime Taskforce -** Organised crime gangs are targeting vulnerable people at home and in the care sector during the COVID-19 crisis, the Scottish government has warned. Justice Secretary Humza Yousaf described the tactics as "abhorrent, but not unexpected". Mr Yousaf, who chairs Scotland's Serious Organised Crime Taskforce, has urged the public and businesses to be alert to gangs looking to "exploit their fears and concerns". The government and police taskforce has now issued official guidelines on how to spot and report suspicious activities. • **Crypto-jacking** - Another issue to be aware of as we all continue to work much more with technology is "crypto-jacking". This is the unauthorised use of a computer, tablet, mobile phone, or connected home device by cybercriminals to steal cryptocurrency like Bitcoin. Hackers trick victims into downloading a malicious file that forces their computers to mine for this money which can be turned it into mainstream cash. Victims may receive a legitimate looking email that encourages them to click on a link, or visits a website infected with malware or when an infected advert pops up malicious code automatically runs. • **Google Scam Spotter -** Google has launched a new website called Scam Spotter. Google has partnered with the Cybercrime Support Network and says this will help people identify and avoid common scams on the internet. The website teaches the three golden rules of scam spotting: 'Slow it down, Spot check and Stop! Don't send'.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			• **Revolut Card Scam** - Revolut customers targeted with scam texts and malicious Google ads. Consumer rights organisation Which? first reported a malicious Revolut ad in March, but this attack has recently resurfaced, leading to one victim losing almost £8,000. Fraudsters paid for a Google ad posing as digital bank to trick victims into giving away personal details or transferring money. There has also been an increase in phishing texts – all sent to Revolut customers last week – that invite the recipient to click on a link to a scam website. If you bank with Revolut, watch out for similar texts and never click on links within messages. You should contact Revolut via the in-app chat function. If you think you've been scammed, you should contact your card provider immediately and report this crime to Police Scotland on 101. Forward scam texts to 7726. • **WHO Impersonators** - Google has noticed an increase in spoofed accounts impersonating the World Health Organisation. These accounts, often made by hack-for-hire criminal organisations, are being used to target businesses and healthcare organisations in the US and UK. The scams are similar to those seen before where the email poses as a way to get up-to-date information on the pandemic. However many of these sites now contain logins to attempt to phish user credentials. NCSC have guidance to help you spot the most obvious signs of scam emails and what to do if you've already clicked. • **DVLA & TV Licence** - DVLA scam text messages are sent to thousands of motorists with officials warning customers not to click on any links or share any personal information. DVLA do not send texts or emails about vehicle tax funds nor would they ask you to confirm your personal details or payment information. DVLA is reminding customers that the only official place to find their services 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**
			information is on GOV.UK. Cyber scams are common, so they have put together some helpful tips online to help customers to spot fraudulent activity. Following on from last week's Bulletin, the public are being warned about a fake TV Licence email. Recipients are told that they are eligible for a "COVID19 Personalized Offer" of six months free. The messages contain links to genuine-looking websites that are designed to steal personal and financial information. Always question unsolicited requests for your personal or financial information in case it's a scam. Never automatically click on a link in an unexpected email or text, instead visit the website direct. **For more information and what to do to reduce the risk view Cyber Resilience Notice - 04 Jun 2020**
28 May 20	**Scottish Business Resilience Centre**	https://abc11.com/nc-attorney-general-josh-stein-better-business-bureau-covid-scams/6215201/ https://www.enterpriseai.news/2020/05/27/contact-tracing-apps-attracting-hackers/ https://www.theregister.co.uk/2020/05/27/criminal_services_cheaper/	**Contact Tracing Dangers -** With contact tracing solutions being launched around the country, experts have warned of the risk of increased phishing emails, texts and phone calls from fraudsters impersonating contact tracers. As the contact tracing systems are new, not much is known about the nature of the communications an individual will receive if they have been on contact with an infected individual. What is clear is that the NHS will never contact you and get you to click on a link with a sense of urgency, which is a common tactic for malicious users. Individuals should be cautious when reviewing emails and texts regarding contact tracing. **Hacking Services Become Cheaper -** A Trend Micro paper has shown over the past 5 years hacking services like botnet rentals or buying stolen credit cards have become cheaper. The paper details that as it becomes easier for hackers to perform the services, the prices for these services and products is reduced. An example used to detail this is that in 2015, a stolen, low balance credit card could be bought for

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			around $20, but in 2020, will sell for around $1.
28 May 20	**Trading Standards Scotland** latest scams across Scotland.	Scam Share - Bulletin 11	This Bulletin highlights: • **Fake Online Stores -** With consumers having to purchase more products online due to the lockdown, scam online stores are becoming more common. These websites offer high-demand items at cheap prices and go to great lengths to look like legitimate businesses. There have been several complaints recently from Scottish consumers who have bought sportswear, gardening equipment, clothing and electrical goods from online stores which may be fake. The fake online stores appeared to be based in the UK had professional-looking websites. Consumers did not receive any confirmation of their orders and have still not received the products they paid for. In all cases, the companies are not replying to emails or phone calls - in one case, the company has removed their phone number from their website. • **Fake Electrical Products -** With hairdressers and barbers still closed, Electrical Safety First have this week warned of the dangers of buying hair clippers and other electrical beauty products through online marketplaces such as Amazon and eBay. An investigation discovered several salon products such as hair clippers which did not meet UK safety standards, and which could have posed a risk of fire or electric shock. Some of the items were being sold with travel adaptors rather than UK plugs, while others had plugs which were dangerously small, and which are illegal in the UK. • **COVID-19 Phone Scams -** There were reports from Scottish consumers this week about fraudsters posing as police officers who had phoned them to tell them that they had breached COVID-19 restrictions and would have to pay a fine. Police

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 have advised that "only criminals will try to rush or panic you" and have urged the public to be wary of phone scams related to COVID-19. In another recently reported phone scam, an unsolicited caller quotes misleading statistics about COVID-19 deaths in an attempt to sell overpriced face masks, gloves and hand sanitiser. A user of the Neighbourhood Watch Alert system this week reported an automated call which told them that they had committed tax fraud and that they would be arrested unless they pressed 1 to speak to an adviser. Find out more about common HMRC scams on our website. • **Warranty Scams -** Scottish consumers have recently reported unsolicited calls saying that the warranty for their washing machine needs renewed. • **Ongoing Advice: Working From Home -** It was reported this week that there has been a significant rise in the number of cyberattacks targeting people working from home. The increasingly sophisticated attacks include fake invitations to Zoom meetings, 'spoofing' attacks where emails appear to come from trusted colleagues or IT departments and scam emails telling business employees that they can choose to be furloughed by signing up to a particular website. • **Collapse of Specialist Leisure Group -** Following the collapse of Specialist Leisure Group, seven Scottish hotels have stopped trading this week, leading to 64,000 cancellations. The majority of these bookings were protected by ATOL or another scheme and will be refunded. However, some individual bookings may not be financially protected. The Specialist Leisure Group operated several businesses - find all of the companies affected here. • **False Medical Claims -** This week, the Advertising Standards Agency has banned social media adverts by a former Apprentice contestant's company, which

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			suggested that their Vitamin C sachets could help to cure COVID-19. Similar adverts can be reported to the ASA using their online form. As home testing kits for COVID-19 become more widely available, it is vital that consumers understand what they are buying. One Scottish consumer reported this week that they had paid for a COVID-19 immunity test, believing that it had been medically approved. However, they then discovered that the test was not in fact approved due to the blood collection method used. • **Ongoing Advice: Supermarket Voucher Scam -** Last week, we discussed a Lidl voucher scam, where consumers were asked to fill out a survey on social media in order to win a £175 voucher. This week, there have been complaints about scam emails which seem to be from Tesco, saying that they are having a prize draw to win vouchers and asking you to click on a link to enter. • **Ongoing Advice: Illegal Puppy Trade -** It was reported this week that demand for puppies in the UK is soaring, as more people are furloughed or working from home. This has led to price increases and long waiting lists for several in-demand breeds. The Dogs Trust charity has warned that this high demand could lead to an increase in illegal puppy farming - a business often run by criminal gangs. • **Ongoing Advice: Doorstep Scams -** Police Scotland have reported a 10% rise in fraud-related crime since 24th March, with many criminals exploiting anxieties and uncertainty around the COVID-19 pandemic and lockdown. Download our 'No Cold Calling' leaflet for advice on shutting out scammers and remember that you are not being rude if you shut the door on unsolicited callers. **For more information and What to Do view Scam Share - Bulletin 11**

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
28 May 20	**Scottish Government Cyber Resilience Unit -** Sharing important information and guidance on COVID-19 related scams.	Cyber Resilience Notice - 28 May 2020	This Notice highlights: • **Easy Jet Data Breach -** Last week's Bulletin contained information following EasyJet's notification of a data breach. If you have been affected, you should have been contacted this week, most likely by email. If affected, you should consider following the advice set out by NCSC. Regardless of the company you've booked with, individuals should be aware of fake websites and emails purporting to offer refunds for holidays cancelled due to COVID-19. • **Downloading apps -** There are millions of apps available to download onto smartphones and tablets that can range from location-based discovery tools and smart search, to games and exercise tracking. Almost all smartphones come with a location-sharing app like Find My Friends that lets you connect with other people's phones, or location tagging on social media apps like Facebook, Instagram, Snapchat and Twitter. By posting where you are, anyone can track your movements (See Resilience Notice for **Top Tips**). The Information Commissioners Office (ICO) is the UK's independent body set up to uphold information rights. The ICO have created a number of resources to help you understand your rights with regards to your online data. They provide guidance on social media privacy settings and factsheets on some of the most popular social media platforms (Facebook, Twitter, Snapchat, LinkedIn and Google) to assist you in taking control over how your personal information is used. • **Ongoing Advice: TV Licensing Scam -** Police forces across the UK have warned of a new scam around TV licensing. The scam impersonates the TV Licensing company, demanding that users give their bank details to make a payment or face prosecution. The scammer also suggests that the user may be entitled to a

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			discount or partial refund due to the coronavirus. The official TV Licensing Company has released a statement saying they will never email individuals with refund or discount offers. Further, they have put a up a page with FAQ on TV Licensing during COVID-19 which states that they are currently not writing to people behind on their license fee payments during the pandemic. TV Licensing have email security and scam advice on their website, including four quick ways to spot a scam. You can also view your licence or payment plan online. • **Voucher Scams -** There are a range of 'offers' circulating online. North Wales police have warned of a scam WhatsApp message circulating where scammers are impersonating Domino's Pizza. The scam contains a malicious link that users click to allegedly receive free pizzas. Domino's Pizza do not offer vouchers through links and only offer voucher codes. If you receive this text don't click on any links. You can forward the texts and any other scam texts to 7726 (the numbers spell "SPAM" on your keyboard). **For more information and what to do to reduce the risk view Cyber Resilience Notice - 28 May 2020**
25 May 20	**Police Scotland** Moving your business from the physical to the digital Sole traders, Self-employed, Small and Medium Sized Organisations	https://www.gov.scot/collections/coronavirus-covid-19-guidance/	Due to the COVID-19 pandemic and the temporary closing down of high streets stores and offices, businesses are adapting the way they operate with many moving to an online model including online shopping, working from home and conferencing software to keep in touch with staff. This is in addition to guidance provided by the Scottish Government. Cyber criminals are aware of these changes in working practices and are trying to take advantage of any possible cyber security weaknesses. Businesses transitioning from high street to online or expanding their online presence should not only consider how they make this change to online trading; but also consider cyber security measures

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			they need to implement to protect themselves. The National Cyber Security Centre has issued advice for these businesses who have seen their physical premises closed and have moved their operations online.
21 May 20	**Trading Standards Scotland** latest scams across Scotland.	Scam Share - Bulletin 10	This Bulletin highlights: • **Counterfeit Goods Online -** Many products, such as sports equipment and clothing, games, games consoles and other electronic products are still in high demand due to the lockdown and are difficult to source online. The BBC recently reported that an online gadget store selling hard-to-find items was appearing at the top of Google searches for products such as cross trainers, newly released games and games consoles. It is believed that this was a scam store and it has since been removed from Google's search listings. Several consumers have reported losing hundreds of pounds after purchasing items through this website which they did not receive. The main warning signs indicating a scam website were: ➢ Many of the items were significantly cheaper than in official stores, where they were sold out; ➢ Customers were asked to pay by bank transfer rather than by credit/debit card; ➢ The website contained several spelling and grammar errors; ➢ The site was less than a month old and was registered to a UK address which belonged to a completely different company. • **Council Tax Scams -** Scam emails and texts telling you that you are due a council tax reduction are yet again becoming more frequent. A recent example shows the start of the link to look like it will lead to an official Government website, it ends in .ru/x/ • **TV Licence Email Scam -** There have been several recent reports of a new scam

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 telling you that your TV License has expired or that your Direct Debit payment has been declined. The email may say that you are entitled to a special offer of six months free. You are asked to click on a link to update your payment details, which will take you to a fake website with official-looking branding where you will be asked to enter personal and banking details. • **Ongoing Advice: IPTV - Illegal Streaming -** FACT reported this week that their online scanning team removed more than double the volume of film links and illegal streams in April, compared to February. The number of downloads for some recently released films has trebled. • **Ongoing Advice: Business Grant Scam** - In the bulletin, we have previously featured scam emails related to COVID-19 business grants - a further example was recently received by a business. The email says that the business has been awarded a Retail, Hospitality and Leisure Grant for £25,000. It states that the payment will not be processed until the link is clicked to start the application. The email looks legitimate, with official Gov.UK branding; however, clicking on the link will lead to a fake Government website asking you to enter business and financial details. • **Ongoing Advice: Supermarket Voucher Scam -** A few weeks ago, we reported that scammers were emailing fake vouchers, supposedly from supermarkets, offering assistance buying food. Clicking on the link to apply for the coupon could take you to a site trying to steal your personal and financial details. This week, a similar scam has been reported - this time, consumers are being encouraged to click on a link on social media to fill out a survey in order to win £175 of Lidl vouchers. Lidl have confirmed that this is a scam.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			• **Stay Safe Online** - Consumers across Scotland are being bombarded with increasingly sophisticated email and cyber scams as they work, socialise and educate their children online. The National Cyber Security Centre this week published details of a survey which found that only 9% of employees working from home had checked whether their anti-virus software had been updated and that only 23% had received guidance on using video conferencing tools safely. • **Ongoing Advice: Doorstep Scams -** Despite the lockdown, rogue traders 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 scams are continuing. • **Ongoing Advice: PPE and Medical Products -** As the first face-mask vending machines appear in the UK, consumers should remain wary of masks or face coverings being sold through online marketplaces or from unknown sellers which claim to be PPE or to offer medical-grade protection. Counterfeit or poorly made masks may offer a false sense of security and may not provide the advertised level of protection. Vistalworks have published a blog with advice on how to navigate the increasing number of face coverings available to purchase online. Consumers should remain wary of any medical claims made by PPE sold by unofficial sources. • **Deliveries -** Scottish consumers are still regularly reporting issues with deliveries during the COVID-19 pandemic. Remember: your consumer rights have not changed due to the COVID-19 pandemic. Find out more information from the Delivery Law UK website or from Which? and if you have experienced problems with deliveries, contact Advice Direct Scotland, who have detailed information about your consumer rights on their website.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			• **Ongoing Advice: Travel Advice -** View the Scam Share Alert for the most recent guidance and advice on travel/accommodation. **For more information and What to Do view Scam Share - Bulletin 10**
21 May 20	**Scottish Government Cyber Resilience Unit -** Sharing important information and guidance on COVID-19 related scams.	Cyber Resilience Notice - 21 May 2020	This Notice highlights: • **EasyJet -** confirmed this week that it had suffered a cyberattack and is in the process of contacting affected customers following the incident. It said email addresses and travel details had been stolen and that 2,208 customers had also had their credit card details "accessed". If you're an EasyJet customer see the Cyber Resilience Notice for recommendations. • **Microsoft** - According to Microsoft, new phishing campaigns are using COVID-19 lures to trick recipients into opening malicious attachments. Threat actors pretend to be from, for example, the Centres for Disease Control (CDC) offering the latest information on the virus and a new "BUSINESS CONTINUITY PLAN ANNOUNCEMENT STARTING MAY 2020". • **Ongoing Advice: Bitcoin Scam -** Reports are coming in about emails promoting Bitcoin investment scams, claiming to take advantage of the financial downturn and helping people recover from bankruptcy. Fraudsters are using images of celebrities to make the emails seem authentic, but in reality, the celebrity has no knowledge of the scam and does not endorse it. Always question unsolicited requests for your personal or financial information. • **Romance Scams -** Organised criminals will be exploiting loneliness during lockdown to take money from romance scam victims. Cyber criminals "meet" people on dating sites, then take the conversation onto private messaging, build up a picture of their victim, then take any opportunity to steal money from them.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			Criminals who commit romance fraud trawl through profiles and piece together information such as wealth and lifestyle, in order to manipulate their victims. Never send money to someone online that you have never met. **For more information and what to do to reduce the risk view Cyber Resilience Notice - 21 May 2020**
14 May 20	**Trading Standards Scotland** latest scams across Scotland.	Scam Share - Bulletin 9	This Bulletin highlights: • **Illicit Puppy Trade -** It may seem tempting to buy a new puppy during the lockdown period. However, Scottish consumers have been reporting puppy-related scams online in recent weeks. In one case, a woman paid a deposit for a puppy which was advertised through an online marketplace. There was an agreement made with the seller that a viewing would take place once the lockdown was lifted and that the puppy would be collected in July. Although the seller seemed legitimate and even sent screen shots of bank account details, they stopped all contact once the deposit had been secured. The consumer did some research into the seller and discovered that they were advertising similar puppies across seven different Facebook accounts. Action Fraud have reported that 669 consumers lost a total of almost £300,000 in March and April after putting down deposits for pets they had seen advertised on social media and online marketplaces. Download our new PDF with top tips on buying a puppy safely online or visit our website for further guidance and links to trusted sources. • **Face Coverings and PPE -** There have been reports by Scottish consumers this week about cold calls offering face masks, gloves and hand sanitiser for £29.99. The caller quoted some misleading statistics about COVID-19 deaths in an attempt to scare the consumer and claimed that 'normal masks' weren't as effective as the

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			ones they were selling, before asking for bank details. The CTSI have reported another similar phone scam, where an automated message says that the wearing of face masks is now obligatory, in an attempt to encourage the consumer to purchase an overpriced mask. The current Scottish Government guidance on face coverings is that: "there may be some benefit in wearing a facial covering when you leave the house and enter enclosed spaces." Their use is NOT currently obligatory and if this changes, it will be reported by the Scottish Government. • **Warning About 'Free Trials' -** The CMA and ASA are reminding people to take care when signing up to 'free' trials. Many businesses are offering 'free' trials of goods and services during the lockdown period, but the terms and conditions of the trial can be unclear, and consumers may not fully understand what they are signing up for. They have compiled some top tips to help you avoid unwanted and unexpected charges which could cost a lot of money. • **Contact Tracing App Scam -** The CTSI have seen evidence of a scam text connected to the UK Government's new contact tracing app for COVID-19, which is currently being tested before being released nationally. The text says that you have come into contact with someone who has tested positive or has shown symptoms for COVID-19. You are asked to click on a link to find out more information - this link leads to a fake website which will ask for your personal or bank information. Consumers who are not on the Isle of Wight cannot currently download the app - once it is available nationwide, users will receive alerts through the app itself. • **Cadbury Hamper Scam** - Consumers have recently reported scams where a competition to win a Cadbury's hamper is advertised through WhatsApp 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**
			Facebook. In some versions of the scam, you are asked to fill out a survey in order to receive a free hamper and to share the link with your friends. One Scottish consumer reported this scam to Advice Direct Scotland, saying that they had been taken in by the legitimate-looking competition and had entered their name, date of birth, mobile number, email address and postal address into the online form. Cadbury has stated that these competitions are scams and that any genuine competitions or giveaways will be advertised through their official website. If you receive a link to take part in this competition or giveaway, do not enter any personal details as they could be harvested by scammers. • **Fake Medical Products -** The Medicines & Healthcare Products Regulatory Authority (MHRA) have again warned the public about medicines and other medical products being sold online claiming to treat or prevent COVID-19, including 'miracle cures', antiviral misting sprays and herbal remedies or vitamins. Their 'Yellow Card' website allows the public to report any suspected side effects from medicines or medical products relating to COVID-19 treatment. • **Travel Advice -** The UK branch of the European Consumer Centre is experiencing its busiest ever month due to a huge increase in consumers seeking advice about airline flight cancellations. Across the whole European network, there were 17,600 queries in April, almost double the number received at the same time last year. View the Scam Share Alert for the most recent guidance and advice on travel/accommodation. • **Charity Scams -** Scammers are taking advantage of the public's desire to support charities during the COVID-19 pandemic by setting up fake websites or posing as legitimate charities who are fundraising to help victims of COVID-19 or to support

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			health services. Consumers are also receiving emails, phone calls and visits from fraudsters posing as charity workers. Charities themselves have also been warned by Police Scotland to 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 changes to a direct debit, standing order or bank transfer mandate in order to direct future payments to a new bank account, which is often run by fraudsters. These requests often appear legitimate – as well as emails, fraudsters can send genuine-looking letters or make phone calls impersonating a genuine supplier. • **Stay Safe Online -** Consumers across Scotland are being bombarded with increasingly sophisticated email and cyber scams as they work, socialise and educate their children online. Since the launch of the National Cyber Security Centre's Suspicious Email Reporting Service two weeks ago, they have received 160,000 reports from consumers about suspicious emails, which have led to the blocking of 300 fake websites. • **Guidance for Businesses -** There has been no change in the law in Scotland for businesses. Businesses that were required to close during the lockdown period are still required to remain closed in Scotland. • **Ongoing Advice: Doorstep Scams -** If you need to call a trader for emergency repair work during the quarantine, find someone who has been vetted and approved through a national or local authority trusted trader scheme. **For more information and What to Do view Scam Share - Bulletin 9**
14 May 20	**Scottish Government**	Cyber Resilience Notice - 14 May 2020	This Notice highlights: • **Online Gaming -** Children and young people are spending so much more time in

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
	Cyber Resilience Unit - Sharing important information and guidance on COVID-19 related scams.		the virtual world, chatting, viewing, sharing and gaming. Cyber criminals are upping their game and altering their methods to attack and disrupt all our lives. As parents and carers, we have to remain vigilant and be aware of potential dangers online. Remember, unless you know who you are communicating with people can pretend to be whoever they want to be online. People can easily hide their true identity, so don't just trust anyone you meet online. Make sure you know who they are and, if you're not sure, just stop communicating with them. If anyone makes harmful suggestions or tries to share indecent images, report the incident to Police Scotland on 101, or 999 in an emergency. • **Interpol -** has launched a global awareness campaign (running from 4 to 31 May) to keep communities safe from cybercriminals seeking to exploit the outbreak to steal data, commit online fraud or simply disrupt the virtual world. The key message of the campaign, which focuses on alerting the public to the cyberthreats linked to the coronavirus pandemic, is to #WashYourCyberHands - to promote good "cyber hygiene **For more information and what to do to reduce the risk view Cyber Resilience Notice - 14 May 2020**
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

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			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 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

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 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 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

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			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**
07 May 20	**Scottish Government Cyber Resilience Unit -** Sharing important information and	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

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
	guidance on COVID-19 related scams.		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 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

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			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**
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

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			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. • 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. **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.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			• **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. "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."

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			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 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

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			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 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

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			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. • 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

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			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** Get Safe Online 'Safe email' 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

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			'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 Cyber Resilience Notice - 30 April 2020**
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

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			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 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

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			'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-19 related scams.	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 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

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			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). **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**	Scam Share - Bulletin 5	This Bulletin highlights: • **Online Shopping -** When shopping online, carry out some research before

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
	Standards Scotland latest scams across Scotland.		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, 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

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			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 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	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

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
	important information and guidance on COVID-19 related scams.		**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 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**

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
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. • **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

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			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 reduction 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. • 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

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			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. • 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.

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 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. ➢ 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

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 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**
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.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			• 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, 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

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			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. • **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

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			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.
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.

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
			For more information and What to Do view TSS Scam Share - Bulletin 2
19 Mar 20	**Trading Standards Scotland** latest scams across Scotland.	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 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**	CFS Intelligence Alert: 10 2019/20	• **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.**

Table 2: Protecting NHS Scotland members of staff and their families from fraud during COVID-19			
Date	**Topic**	**Links to Sources**	**Advice and Guidance**
	Advice to help NHS members of staff to protect themselves against increased social media scams	UK Action Fraud Sophos	• **Beware of Gift Cards** - Links are shared via social media to a giveaway of free 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.

Glossary

Phishing	Phishing is a mirror image of the Smishing style attempt, but Phishing is used in emails. They have a very similar structure encouraging the recipient to click on a hyperlink in the email which can either take you to a fake website, or more concerning download malicious software onto your device.
Ransomware	Ransomware is a type of malware. It lets hackers take control of a company's systems and encrypt their data, demanding payment to release it. It is often sent via a malicious email link to employees. This type of cyber-attack is not uncommon.
Smishing (SMS Phishing)	Smishing is an attempt by fraudsters using SMS text messaging. These texts can bait the recipient encouraging them to click on links, that in this case are offering financial incentives—including government payments and rebates (such as a council tax rebate)—as part of the lure. The Coronavirus is also being used by cyber criminals in related **Phishing** attempts trying to exploit you with similar fake financial support packages and rebates. In addition to SMS (Texting), other possible ways of **Smishing** include contacting you on other messaging apps you might use. If you respond to these attempts, you could lose money and risk your identity being stolen. So, be alert to this and report suspicious texts by **forwarding the original message to 7726**, which spells SPAM on your keypad.

Spoofing (email)	Email spoofing is how fraudsters send emails that look like they have originated from genuine email accounts. The email “From” header appears legitimate, when in fact the genuine owner of the email account knows nothing about it.
Threat Actor	A threat actor or malicious actor is a person or entity that is responsible for an event or incident that impacts, or has the potential to impact, the safety or security of another entity. Most often, the term is used to describe the individuals and groups that perform malicious acts against organizations of various types and sizes. From a threat intelligence perspective, threat actors are often categorized as unintentional or intentional and external or internal.