CURRENT SCAMS – MAY 2021

Scam texts can be forwarded to Ofcom via 7726 and emails to Cyberawaregov which has launched SERS – the suspicious email reporting service. If you receive an email which you are not sure about, please forward it to **report@phishing.gov.uk** There is further information on the website: **www.ncsc.gov.uk/information/report-suspicious-emails**

If you think you have been a victim of fraud you should report it to Action Fraud, the UK's national fraud reporting centre by calling 0300 123 20 40 or by visiting **www.actionfraud.police.uk**

Action Fraud have advised on a British Gas scam via email. It states: "Hello, British Gas wants to inform you that you are eligible for a payment refund of £594. "Our records indicate that you have paid more than you should have for your British Gas Service from 2017-2019 and because of this reason, we have decided to refund you the total amount which you have overpaid." There is also a link within the emails, which the fraudsters hope recipients of the email will click. Further details in the below link: **British Gas scam sees hundreds receive fake refund emails 'designed to steal' bank details (msn.com)**

Warnings have been issued about a scam which appears to offer you a free Dyson vacuum cleaner from Curry's but could in fact give fraudsters access to your bank account. The fake message tells customers they've been chosen to win a free Dyson vacuum cleaner and asks for your credit or debit card details to cover a £1 delivery charge. If you hand over your details you could lose thousands of pounds. An email purporting to be from Dyson is promising 'prizes' as part of a fake loyalty program. Dyson has confirmed it has nothing to do with the communication. Further details in the below link: **Warning issued over free Dyson scam emails which could empty your bank account - Mirror Online**

Major mobile networks including EE, Vodafone, Three and O2 are warning customers about a new text message scam. The message, which pretends to be from delivery firm DHL, asks users to install a tracking app - but it's actually a form of malware. Known as Flubot, it can take over your device if you click on any links to gather personal data, including online banking details. It can also eavesdrop on incoming notifications, read and write SMS, make calls and transmit your entire contact list back to its contact centre.

Vodafone said millions of the text messages have already been sent across all networks, and it's now urging customers to be "especially vigilant". It's also telling users who've received the messages and clicked on the links to stop using the device, reset it to factory settings and restart it. By forwarding any suspicious text messages to 7726, which is a free reporting service run by telecoms regulator Ofcom, the links can be tracked. Once you've reported it, it is best to delete the message from your phone. Further details in the below link:
Millions of EE, Vodafone and Three customers warned about fake text message scam (thesun.co.uk)

Phone companies must do more to stop fraudsters who spoof phone numbers to trap victims, one of the UK's top law enforcement officers has said (click on link to read this article): https://www.bbc.com/news/business-56521518

The Amazon Prime scam involves victims receiving an automated call informing them that they have been charged for an Amazon Prime subscription and to press 1 to cancel the transaction. There are also other Amazon scams circulating at the moment. **Do not press 1 or any other number mentioned on any of the automated scams. There is also a new Amazon scam asking you to purchase 3 Amazon vouchers for somebody you know. Please click on this link to Which article to read all about this nasty and complex scam: Scam alert: Amazon gift card COVID-19 email requests – Which? Conversation**

HMRC automated phone call scam which will tell you that they are filing a lawsuit against you, and to press 1 to speak to a caseworker to make a payment. If you receive such a call, please put the phone down immediately. The callers use a variety of numbers and HMRC would like you to report full details of the

scam by email to **phishing@hmrc.gov.uk** including date of the call, phone number and content of the call. Also, texts have been received purporting to be from HMRC advising that you have a tax rebate and emails with the wording "that if you're self-employed or a member of a partnership and have been impacted by coronavirus (COVID-19) you are eligible to claim a grant. Government is giving a grant between 2,500 pounds and 7,500 pounds if you are a tax payer. You must download the form attached to this email and fill out the required information to complete approval for your grant claim." **SEISS fourth grants will soon be rolled out and self-employed workers will be able to make a claim from late April onwards. Unfortunately, scammers have looked to take advantage of this and workers have been urged to look out for suspect emails claiming to be from HMRC.**

Residents are receiving an official-looking email headed Council Tax – Gov.uk advising that you are getting a Council Tax Reduction (this used to be called Council Tax Benefit) considering you`re on a low income or get benefits. Apply now to claim the reductions made over your past 5 years of Council tax payments and they may quote total amount of benefits as £385.50 and that the refund will be transferred direct to your Debit/Credit Card. Do not click on any of the links as they are just trying to obtain your card details.

Royal Mail customers are being warned about a new convincing scam email that has been circulated. It is asking people to pay £2.99 fee for an undelivered item of mail - but while the sum might seem small, what the criminals actually want is bank account details and they have then emptied their bank account! The message, which appears at first glance almost genuine, warns homeowners if they don't opt for delivery, they will return the package to the sender. It then directs the customer to a link, asking them to fill out an information form. The form then asks users for their card number, security code, sort code, account number and mother's maiden name. **Also, similar scams purporting to be from Hermes, DPD and DHL asking for delivery payment.**

Letters are being received purporting to be from Klarna advising that a payment has not been received and requesting settlement via a website and asking you to use the quoted log in details. Klarna is quite a well-known genuine provider of short-term finance and their letter is sadly being used by Scammers.

Fake messages inviting Asda and Morrison's customers (and possibly more Supermarkets) to track their grocery delivery. Scammers are sending these texts to phone numbers on the off chance the recipient has placed an order and again this is another trick to access banking information. People worried about deliveries should check directly with the stores.

Fraudsters are known to make calls claiming to work for BT, when it's actually a scam. They may ask you for personal information, want access to your computer and in some cases, ask for your bank details. **Also calls purporting to be from Microsoft and asking for your Licence number which they would know, so please do not fall for this scam.**

Letters from International FIFA World Cup Online Lottery informing residents they have won £825,000 is a scam and includes numbers to phone to claim the prize.

Halifax, TSB, Lloyds, HSBC and other banking scams are being sent by text, automated phone call or email, so do not respond and always go to the genuine websites or phone your bank if you wish confirmation that this is a scam. **Texts also from HSBC asking you to approve a new payee request.** People who use online banking have been warned about a new scam appearing to be from HSBC. The text message states a new payee has been added to your account and to call them up on the number provided if you did not make this request. People who call this number could be put in touch with a scammer who attempts to gain your personal details in order to take money from your bank account. The message has been sent by a regular-looking phone number which does not label HSBC as the sender.

Accident calls are still being received in the hope that you may have had an accident. **Also DVLA Scams advising that your car appears to be untaxed or they have mislaid your details** and that a fine of £1000 will

be made if you do not send details. The fact that the registration number is not shown on the e-mail is proof that it is a scam so do not reply to any requests.

Residents are still receiving calls from the Insulation Advisory Line saying that they need to check your loft insulation for mould. The STD code comes up as from Leeds but shows it as an International call when the phone rings. Do not arrange for them to visit and check.

Phone calls are being received from a group who call themselves "Security Advisers" and wish to carry out a security review on your property. Other companies have used this ploy in the past to arrange a visit and then advise that you need additional security such as alarms or CCTV. They often say that if your alarm is activated it goes straight through to the Police but this is untrue and may say that the security system is free but then you pay extortionate costs for their monitoring service.

NHS scams. There are still variations of these by phone, text or email, so please be careful not to give any Bank details. One of the latest scams involves the caller saying that they are from NHS and ask a few health-related questions. They then proceed to ask if you have a life insurance which they try to sell you if you do not have one currently. Another extremely dangerous scam is calls with fake vaccines or tests being offered and you will be asked to pay for these and they will again be after your bank details.

National Insurance Scam. Victims have reported receiving an automated telephone call, during which they are told their "National Insurance number has been compromised". They are then instructed to "press 1 on their handset to be connected to the caller" in order to supposedly fix the issue and get a new National Insurance number. Once connected to the "caller", victims are pressured into handing over personal details - which the fraudsters claim is to enable them to receive a new National Insurance number. However, giving the criminals your personal details will enable them to commit fraud using your credentials and information.

Angela Money BEM

Neighbourhood Watch