**A brief guide to fraud prevention**

**Between April 2019 and March 2020 there 7471 people reported that they had been a victim of fraud in Humberside. This was up 9% on the year before. The total amount these victims lost was £13.7 million which was up 60% on the year before. In North Lincolnshire there were 724 victims losing £3.2 million.**

**During the COVID period there have been several scams that are aimed at taking advantage of the situation. A number of these are phishing emails sent to unsuspecting victims.**

**Never click on links or download attachments as criminals may infect your devices with malware or ask you to enter your personal or financial information into fake websites. In some cases, this can lead to your identity being stolen.**

**Below are some of the current frauds in circulation**

**Primark Covid-19** - A new Primark phishing scam campaign started in early July 2020. These emails offer the recipient a reward “*on the occasion of overcoming the Corona virus*” and asks them to click on a link to fill out a survey. This link is confirmed as malicious. It is likely that these emails may have been spoofed by the fraudster. They are spoofing the email address of a genuine brand (*contact@primark.com*) to trick the recipients into trusting the origin of the message and get them to open, respond and click on any links within the body of the email message.

**Covid-19 Relief Fund** - These emails are claiming to be from “*LSDSM Organisation*” and they are offering relief funds up to $1,000,000 US dollars to selected individuals, to purchase and distribute relief materials for the control of Covid-19 in their region. Recipients are asked to contact an email address for further information on how to claim this fund. These emails have been sent from a variety of email addresses.

**World Health Organisation Covid-19 Support Group** - This is a new phishing attempt purporting to be from the World Health Organisation (WHO), which first started in July 2020. The emails state they are offering social relief distress grants to selected individuals for the sum of 1,500,000 EUROs because of the outbreak. This is like a previous phishing email that was circulated. The recipient is asked to provide their personal and occupation details via an email address to the WHO Trust Fund and process their claim and receive these payments.

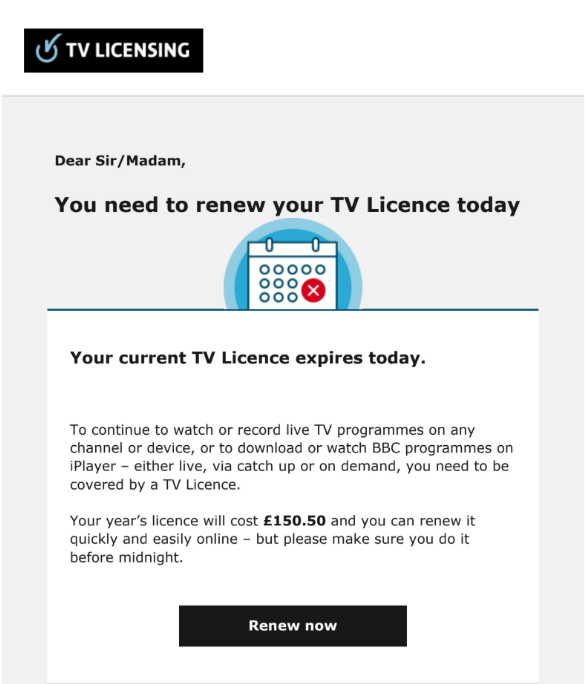
**Coronavirus Job Retention Scheme** - A new HMRC themed phishing scam states that the Government are checking all claims made through the “*Coronavirus Job Retention Scheme*”. These emails display the subject header *“Coronavirus Job Retention Scheme”* and the recipient is asked to respond to the email and provide their personal details including a scanned copy of their National Insurance number. This email look authentic and convincing especially as they contain the HMRC brand logo and has been signed off by the HMRC Compliance Officer. It also comes from a legitimate appearing email address ([*covid19@hmrc.gov.uk*](mailto:covid19@hmrc.gov.uk))

**TV Licensing**

The TV Licensing fee changes for over-75s could mean that you’re contacted by a criminal. You may receive emails and/or texts purporting to be from TV Licensing using the organisation’s official branding to convince you it’s genuine. These messages often claim that your payment has failed and include a link to set up a new direct debit.

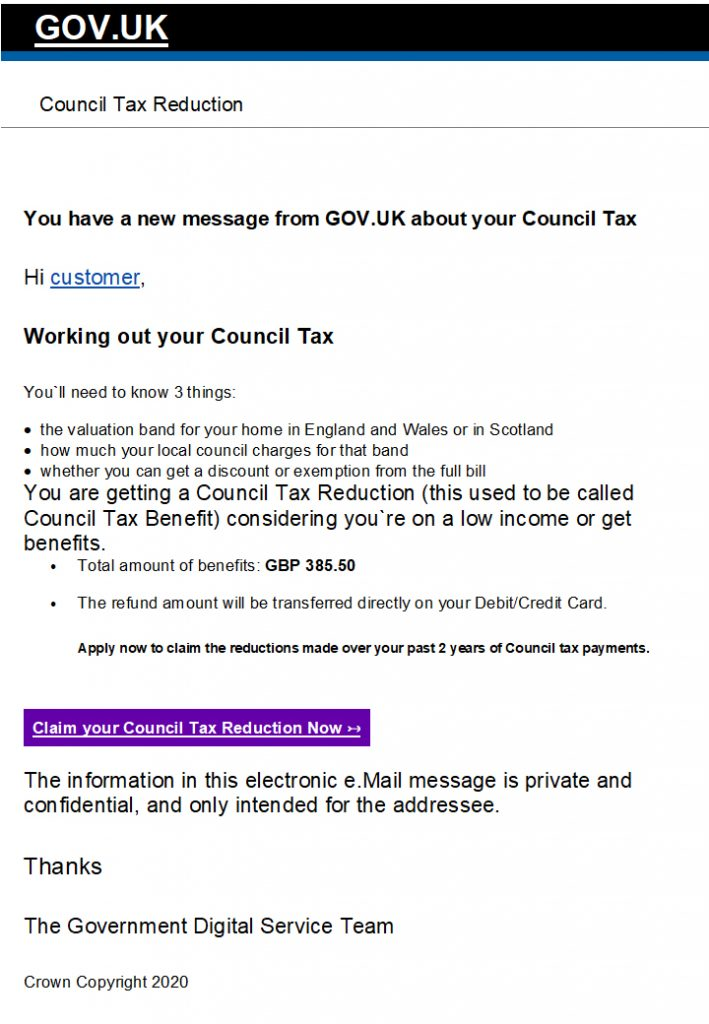
However, you should avoid clicking on links in unsolicited emails as they could lead to fake websites designed to look like that of the genuine organisation but which are in fact set up to obtain your personal and financial information.

Below is an example of a scam email:



**Council Tax reduction**

If you receive an email from a “government department” offering you a council tax reduction then take a moment to Stop, Challenge, Protect. Criminals are using official government branding in emails to convince you they’re genuine and to trick you into giving them your money or information. Emails received often contain links which, when clicked on, lead to an “official looking” webpage designed to access your personal information. In some cases, this could lead to criminals using your identity to commit fraud. Below is an example of a council tax reduction scam email:



**WHAT TO DO IF YOU GET SCAMMED**

**GET HELP AND REPORT A SCAM**

If you think you have uncovered a scam, have been targeted by a scam

or fallen victim, there are many authorities you can contact for advice or

to make a report.

Reporting crime, including fraud, is important. If you don’t tell the authorities, how

do they know it has happened and how can they do anything about it? Remember

that if you are a victim of a scam or an attempted scam, however minor, there may be

hundreds or thousands of others in a similar position. Your information may form part

of one big jigsaw and may be vital to completing the picture.

**Reporting fraud**

All fraud should be reported directly to Action Fraud.

Action Fraud Reporting online: www.actionfraud.police.uk

Telephone reporting: 0300 123 2040

**Unless**

A crime is in progress or about to be committed. The suspect is known or can be easily

identified. The crime involves a vulnerable victim. If this is the case you should contact police directly either by dialling 999 in an emergency, dialling 101 in a non-emergency or visiting your local police station. If you have information on any crime and you would prefer not to speak to police, you can call Crimestoppers anonymously on 0800 555 111 or visit [www.crimestoppers-uk.org](http://www.crimestoppers-uk.org) Crimestoppers is an independent charity.



**NEVER DISCLOSE SECURITY DETAILS** A genuine bank or organisation will never ask you for details such as your PIN or card number over the phone or in writing. Before you share anything with anyone, stop and think. Unless you’re 100% sure who you’re talking to, don’t disclose any personal or financial details. Instead, hang up and contact the organisation yourself using the number on the back of your bank card or on their website**.**

**DON’T ASSUME AN EMAIL OR PHONE CALL IS AUTHENTIC** Just because someone knows your basic details (such as your name and address or even your mother’s maiden name), it doesn’t mean they are genuine. Criminals will use a range of techniques to get your details and may even say you’ve been a victim of fraud to scare you into action.

**DON’T BE RUSHED OR PRESSURED** Under no circumstances would a genuine bank or another trusted organisation force you to make a financial transaction on the spot; they would never ask you to transfer money into another account, even if they say it is for fraud reasons. They will always let you call them back on a number you know is real – if they try and stop you doing this, it’s a fraudster and you should hang up.

**LISTEN TO YOUR INSTINCTS** If something feels wrong then it is usually right to question it. Criminals may lull you into a false sense of security when you’re out and about or rely on your defences being down when you’re in the comfort of your own home. If your gut-feeling is telling you something is wrong, take the time to make choices and keep your details safe.

**STAY IN CONTROL** Have the confidence to refuse unusual requests for personal or financial information. It’s easy to feel overwhelmed when faced with unexpected or complex conversations. Remember that it’s ok to stop the discussion if you don’t feel in control of it. If you’ve taken all these steps and still feel unsure about what you’re being asked, never hesitate to contact your bank or financial service provider on a number you trust, such as the one listed on their website or on the back of your payment card.

If you would like to improve your knowledge of fraud and take steps to prevent yourself from becoming a victim follow this link to the Friends Against scams website. There is an interactive 20-minute online session to help you <https://www.friendsagainstscams.org.uk/>

<https://takefive-stopfraud.org.uk/>