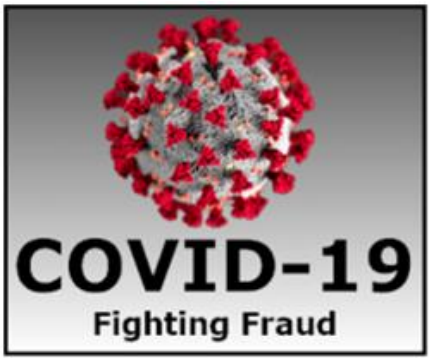

Criminals will use every opportunity they can to defraud innocent people. They will continue to exploit every angle of this national crisis and we want people to be prepared.

We are not trying to scare people at a time when they are already anxious. We simply want to make people aware of the simple steps they can take to protect themselves from handing over their money, or personal details, to criminals.

Law enforcement, the government and industry are working together to protect people, raise awareness, take down fraudulent websites and email addresses, and ultimately bring those responsible to justice.

If you think you have been a victim of a scam, contact your bank immediately and report it to Action Fraud on 0300 123 2040 or via actionfraud.police.uk.

KEY PROTECTION ADVICE

Criminals are experts at impersonating people, organisations, and the police. They can contact you by phone, email, text, via social media or in person. They will try to trick you into parting with your money, personal information, or buying goods or services that don't exist.

If you are approached unexpectedly remember to:

- **Stop:** Taking a moment to think before you part 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 victim to a scam, and report it to Action Fraud.
- You can also report suspicious texts by forwarding the original message to 7726, which spells SPAM on your keypad.
- The police, or your bank, will never ask you to withdraw money or transfer it to a different account. They will also never ask you to reveal your full banking password or PIN.
- Do not click on links or attachments in unexpected or suspicious texts or emails.
- Confirm requests are genuine by using a known number or email address to contact organisations directly.

To keep yourself secure online, ensure you are using the latest software, apps and operating systems on your phones, tablets and laptops. Update these regularly or set your devices to automatically update so you don't have to worry.

What scams are we seeing?

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.

We would remind anyone who receives an unexpected text or email asking for personal or financial details not to click on the links or attachments, and don't respond to any messages that ask for your personal or financial details.

Universal Credit scams

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."

Additional Information:
• For latest information on Universal Credit go to https://www.understandinguniversalcredit.gov.uk/

• We urge people not to click on the links or attachments in suspicious emails, and never respond to unsolicited messages and calls that ask for personal or financial details.

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:

- Impersonating the government and notifying the victim they were due a payment/rebate.
- Incorporating the COVID-19 epidemic into push payment frauds.
- 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.
- Calling purporting to be from the victim's bank, saying their 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.
- Victim persuaded 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.
- COVID-19 used as a hook for offering employment. Victim is persuaded to pay an advanced fee for vetting/qualifications to get them a job which ultimately does not exist.

Phishing/smishing
Some of the tactics being used in phishing emails and texts include:

• Fraudsters purporting to be from a research group that mimic the Centre for Disease Control and Prevention (CDC) and World Health Organisation (WHO). They claim to provide the victim with a list of active infections in their area but to access this information the victim needs to either: click on a link which redirects them to a credential-stealing page; or make a donation in the form of a payment into a Bitcoin account.

• Fraudsters providing articles about the virus outbreak with a link to a fake company website where victims are encouraged to click to subscribe to a daily newsletter for further updates.

• Fraudsters sending investment scheme and trading advice encouraging people to take advantage of the coronavirus downturn.

• Fraudsters purporting to be from HMRC offering a tax refund and directing victims to a fake website to harvest their personal and financial details. The emails often display the HMRC logo making it look reasonably genuine and convincing. There have also had reports of people receiving similar text messages. Also emails purporting to be from HMRC asking them to check their entitlement and make a claim by a specific date to receive any possible repayments. Recipients are asked to click on a link to start a claim.

• Smishing scams claiming to be from .gov.uk. Examples include advising the victim their phone data has shown they have left their home more than once and they should phone a number to pay a fine or risk further punishment. Text messages informing victims they can claim £458 of coronavirus aid. This text features a link to a fake government website, which urges users to enter their postcode to apply for COVID-19 relief.

• Emails stating that Virgin Media is cancelling subscription charges in light of COVID-19. Recipients are asked to click on a link to prevent them from being charged. Other brands, include TV licencing, BT Sport and Amazon.

In addition, fraudsters are sending emails:-

• Selling or giving away face masks, toilet roll, immunity oils etc.

• Shipping or selling COVID-19 testing kits and emergency medical and survival kits at a reduced rate

• Providing health alerts and advice with links on receiving updates and how to avoid the virus

• Encouraging recipients to invest in bitcoin or other financial schemes due to the pandemic's effect on the economy

• Asking recipients to contribute to various COVID-19 related charitable funds e.g. WHO 'solidarity response fund' / Centre for Disaster Philanthropy response fund.