**COVID-19 Fraud and scams**

Action Fraud have seen a number of different scams circulating relating to Covid-19. This includes people falling victim to online shopping scams, believing they are purchasing protective face masks or hand sanitiser, that actually, do not exist. Criminals are also using Government branding to try to trick people, including using HMRC branding to make spurious offers of financial support through unsolicited emails, phone calls and text messages.

Criminals are looking to take advantage of further consequences of the pandemic, such as exploiting people's financial concerns to: ask for upfront fees fraudulently applied to bogus loans; offer high-return investment scams; or targeting pensions.

Huge increases in the number of people working remotely presents an opportunity for criminals to commit computer software service fraud. The increased demand on IT systems causing slower responses may make approaches of help to fix devices seem more believable, when in reality, criminals are trying to gain access to your computer or get you to divulge your login details and passwords. It is also anticipated that there will be a surge in phishing scams or calls claiming to be from government departments offering grants, tax rebates, or compensation.

**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 click on the links or attachments, and don't respond to any messages that ask for your personal or financial details.

**Phishing/smishing**

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

• Criminals purporting to be from HMRC offering a tax refund and directing recipients 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. We have also had reports of people receiving similar text messages. Another MO involves 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. Again, different MOs but examples we've seen 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. In others reports, text messages were sent informing recipients they can claim £458 of coronavirus aid or advising them to click on a link to claim a rebate or grant from the government.

• Emails from courier companies saying a parcel has arrived, and asking the recipient to click on a link and enter details to verify themselves or delivery address.

• 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. We've also seen several reports relating to phishing abuse in other brands, for example TV licencing phishing attempts, BT Sport and Amazon phishing emails.

• Emails being sent to recipient claiming to be from Argos and offering free vouchers to help support people during the outbreak. The email features a link for recipients to claim their voucher.

• Emails, designed to steal personal information, asking parents who still want free school lunches while their child's school is closed, to click on a link and leave their details.

• Emails claiming to be from Hotmail and Microsoft Outlook advising recipient that their account has been deactivated. There is a link for the recipient to verify their details to reactive and secure their accounts. The links provides an opportunity for fraudsters to steal email passwords and personal details. Similar emails advise the recipient that "terms & conditions have changed due to COVID-19" and they need to re-validate their details or their mailbox will be terminated.

**In addition, criminals are sending emails:-**

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

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

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

**Testing/treatment kits**

A Medicines and Healthcare products Regulatory Agency (MHRA) spokesperson said:

"The use of products for the diagnosis of COVID-19 (SARS-CoV-2) infection in community settings, such as pharmacies, or for home use, is not at present advised by Public Health England. We are unaware of any CE marked tests for home use, and it is illegal to supply such products without a CE mark.

"If members of the public think that they have come across a 'Self-Test kit' with CE mark and a Notified Body number, they should contact us and we will investigate, as this product is likely to be fraudulent.

"We are investigating a large number of allegations of non-compliance relating to the selling of medical devices for use during this COVID-19 outbreak. Patient safety is our highest priority so we are looking carefully into all reports on a risk basis. However, we can't comment on individual cases.

"Our advice is always make sure you are buying your medicines and medical devices from a registered pharmacy or website.

"When buying online, beware of bogus websites, suspicious URLS and remember that claims like '100% safe, no side effects' or 'quick results', are often warning signs. Cut prices and speedy deliveries can expose you to fake medicines or devices, identity theft and fraud."

**Universal Credit scam**

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/coronavirus/
- 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.
- We continue to work with Action Fraud and the National Fraud Intelligence Bureau to shut down sites and posts which promote this type of fraud.

**Remember:**

1. 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.
2. 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.
3. 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.
4. If you believe you have been a victim of fraud please report this to Action Fraud.