COVID-19

Fraud Alert

COVID-19 Related Scams

tiaa

During the pandemic there will be fraudsters who try to take advantage of us to make a profit. This Fraud Alert outlines some of the scams that you need to be aware of. Unfortunately, COVID-19 is creating an environment for fraudsters to thrive.

Over the Phone

Fraud: There is likely to be an increase in scam calls, with scammers pretending to be from authorities such as your bank or HMRC. A common phone scam involves receiving a call stating that government guidelines now require everyone to wear a mask outside the home and asks you to "Press 1" to purchase a mask.

Preventative Measures:

- Never give out personal information or log in details over the phone.
- Never agree to transfer money.

Doorstep Callers

Fraud: Scammers are taking advantage of the vulnerable by knocking on doors and offering to do their shopping, provide cleaning services that kill bacteria or pretend to be healthcare workers that provide 'home-testing' for the virus.

Preventative Measures:

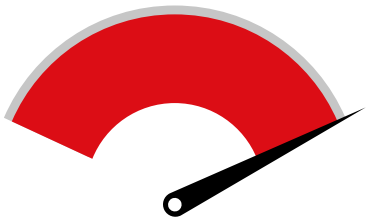
- Never hand over any money to someone you don't know.
- Do not let a stranger into your home.

Online Sales

Fraud: Scammers are also using email to encourage you to buy items such as face masks and hand sanitisers. Once ordered and paid for, the items never arrive.

Preventative Measures:

- Carry out research before making a purchase from a company you don't know.
- Always use a credit card as most card providers insure purchases. Alternatively, use PayPal. If you have lost money, report it to your bank and Action Fraud.



Status: Action Required

This alert provides information and advice to staff about fraud and economic crime that may occur during the COVID-19 emergency, and the risks associated with it.

If you have been scammed, report it to Action Fraud: www.actionfraud.police.uk or 0300 123 2040.

Also, contact your bank if you have lost money.

Action Fraud also provide advice on how to shop safely online: https://www.actionfraud.police.uk/shoponlinesafely

The NCSC provide advice on how to protect your devices from the latest threats: https://www.ncsc.gov.uk/guidance/securing-your-devices

For further discussion and support, including fraud awareness training services, contact:

Jonathan Gladwin, Director of Fraud & Security ■ Email: **covidfraud@tiaa.co.uk**

www.tiaa.co.uk

0845 300 3333

Phishing Emails

Fraud: Action Fraud are reporting an increase in coronavirus themed phishing emails. These emails will try to trick you into opening malicious attachments or revealing personal or financial information. Fraudsters are emailing potential victims purporting to be from research organisations such as the World Health Organisation (WHO), asking you to click on a link for information relating to the coronavirus. The link leads to a malicious website or you are asked to make a payment in Bitcoin. Another scam involves fraudsters purporting to be from the government asking for donations towards the NHS.

In April 2020, the National Cyber Security Centre (NCSC) launched its suspicious email reporting service (SERS), which has resulted in dozens of malicious web campaigns being shut down, following the spike in coronavirus phishing scams. The criminal's goal is to convince you to click on links within their scam emails or to give away sensitive information such as your bank details.

Preventative Measures:

- If you have received an email which you're not quite sure about, forward it to SERS at: report@phishing.gov.uk. The NCSC will analyse the suspicious email and any website it links to. If necessary, they will block the address the email came from and work with hosting companies to remove links to malicious websites.
- Be very wary of unsolicited emails - look out for grammar and spelling errors that are unlikely to be found in legitimate emails.
- Don't be rushed into doing anything - these emails often use an urgent tone, which is designed to make you click on the links quickly. Take your time, slow down the process and consider any actions carefully.
- Legitimate services who you have accounts with will address you by your name, not 'Dear Customer' for example.

Smishing Texts

Fraud: The same applies to SMS messages. Known as Smishing texts, they look like they are from a reputable company, but they will try to get you to act by calling a premium rate number or sharing confidential information. A common smishing scam involves receiving a text message that appears as though it's from the government and asks you to pay a fine, as it says you have been recorded as leaving your home on three occasions during the lockdown - this is fake.

Preventative Measures:

- Don't reply to a text message from someone you don't know and don't click on links within the text message.
- Any apps you install should come from an official app store.

Pet Purchases

Fraud: Criminals are taking advantage of the pandemic to commit fraud involving the purchase of pets, such as puppies or kittens. Victims are putting down deposits for pets they've seen advertised in fake adverts on social media. Scammers use the lockdown restrictions as a reason why the victim cannot see the animal first, or pick it up. After the deposit, more funds are requested to cover insurance and vaccinations.

Preventative Measures:

- Do your research and trust your instincts.
- Choose your payment method wisely - use a credit card or PayPal.

For further discussion and support, including fraud awareness training services, contact:

Jonathan Gladwin, Director of Fraud & Security ■ Email: **covidfraud@tiaa.co.uk**

www.tiaa.co.uk

0845 300 3333