

Common COVID-19 Scams

Important advice on how to avoid falling victim to scams

Free School Meals

Fraudsters are targeting families, emailing parents and carers with messages such as: "If your child is entitled to free school meals send your bank details to the school and they will help with funding while the school is closed". The email contains a harmful link for the parents to follow if they want to receive this funding.

Fake Health Authority Messages

Fraudsters have been emailing individuals, particularly in the healthcare sector using COVID-19 to dupe individuals to hand over personal data.

Charity Donations

Fraudsters are seeking donations for supporting COVID-19 victims, fundraising for a cure or for the NHS.

News/Press Reporting

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.

Fake Payment Update Texts

The recipient is sent a text supposedly by their service/phone/internet provider, informing them that their latest bill could not be processed. The text message asks the recipient to tap a link to update their payment information.

The Good Samaritan

Individuals are offering to do shopping or collect medication and are asking for money upfront and then disappearing.

Fake Officials

Fraudsters are visiting homes posing as police officers and health officials to gain entry to homes of the elderly and vulnerable, promising fake corona virus tests or offering to deliver shopping and other essentials in exchange for money.

Suppliers

Online shopping scams where people have ordered protective face masks, hand sanitiser and other products, which have never arrived.

Mandate/Change of Account

When someone gets you to change a direct debit, standing order, or bank transfer mandate, by purporting to be an organisation you make regular payments to, for example a subscription or membership organisation or your business supplier.

Investments

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. These emails often display the HMRC logo making it look reasonably genuine and convincing.

Medical Treatment/Testing

Claiming a relative has fallen sick with the virus and then requesting payment for treatment.

- Offering people the opportunity to purchase protective equipment such as face masks online which never arrive.
- Offering "miracle" cures for coronavirus are being offered but there is no specific treatment for coronavirus.
- Offering fake home-testing kits for the virus - these kits are not currently available to buy.

Illegal Lending and Loan Sharks

People under increased financial strain may turn to short-term lenders for help. The Illegal Money Lending Team want to help stop Loan Sharks taking advantage of people.
Helpline: **0300 555 2222** www.stoploansharks.co.uk

Report It

Action Fraud (The Fraud reporting centre) and the Police can only know of new scams if you tell them about it. Use Action Fraud's reporting site www.actionfraud.police.uk

Spread The Word

Make sure your friends and family are aware of where to find out about COVID-19 scams. Tell vulnerable members of your family about the scams. Ask them if they have had any contact from potential fraudsters using the scams detailed below. Use Social Media to spread the word about the scams identified by Action Fraud.

Action Fraud website www.actionfraud.police.uk

Follow Action Fraud on Twitter and Facebook
[@actionfrauduk](https://twitter.com/actionfrauduk)
<https://www.facebook.com/actionfraud/>

Re-Tweet scam warnings and share scam posts

Shopping Online

If you're making a purchase from a company or person you don't know and trust, carry out some research first, and ask a friend or family member for advice before completing the purchase. For more information on how to shop online safely, please visit: www.actionfraud.police.uk/shoponlinesafely

Secure your device

Make sure your mobile, tablet, PC and other devices are kept secure. Follow the advice from the National Cyber Security Centre: www.ncsc.gov.uk/guidance/securing-your-devices

Visit 'Get Safe Online' website for advice
www.getsafeonline.org/

Citizens Advice Consumer Helpline 0808 223 1133
www.adviceguide.org.uk

Follow us on twitter and facebook for up to date information on scams

 www.facebook.com/cumbriats/  [@cumbriats](https://twitter.com/cumbriats)

IMPORTANT ADVICE - Keep Your Information Safe

Your bank will never ask you for your PIN number or passwords, and, never ask you to move money from your account into another so-called "safe" account.

Don't click on the links or attachments in suspicious emails or texts.

Never respond to unsolicited messages and calls that ask for your personal or financial details.

The DWP will never text or e-mail asking for your personal details or bank information. HMRC never send notifications of a tax rebate or ask you to disclose personal or payment information by email or text message. You can check a charity's name and registration number at gov.uk/checkcharity



STAY HOME ▶ PROTECT THE NHS ▶ SAVE LIVES