Coronavirus fraud

This document has been approved by the National Economic Crime Centre, Home Office and National Cyber Security Centre.

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 people to be aware of the very simple steps they can take to protect themselves from handing over their money, or personal details, to criminals.

Law enforcement, 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've fallen for a scam, contact your bank immediately and report it to Action Fraud on 0300 123 2040 or via actionfraud.police.uk.

Key protection advice for individuals

Criminals are experts at impersonating people, organisations and the police. They spend hours researching you hoping you'll let your guard down for just a moment.

They can contact you by phone, email, text, on 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 parting 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.

Key protection advice for businesses

Criminals are experts at impersonating people, organisations and the police. They will spend hours researching your business, hoping you will let your guard down for just a moment.

Stop: If you receive a request to make an urgent payment, change supplier bank details, or provide financial information, take a moment to stop and think.

Challenge: Could it be fake? Verify all payments and supplier details directly with the company on a known phone number or in person first.

Protect: Contact your business's bank immediately if you think you've been scammed and report it to Action Fraud.

Keeping your business secure online

Criminals will try and gain access to your device or network, and everything stored on it. They can do this by:

- Sending emails with malicious attachments;
- Exploiting vulnerabilities in your operating systems if they are not up-to-date;
- Trying to get you to click links or visit malicious websites.

Once they have access to your device and your data, they may try to steal your data or extract money from you by getting you to pay a ransom. There are a number of steps you can take to protect your device and operating systems and educate others on your network. Please visit the NCSC website to find out more.

You can also read the National Cyber Security Centre's Small Business Guide: Cyber Security for more advice on how to keep your business secure online.

What scams are we seeing?

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:

- Suspect 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.
- Suspect calling purporting to be victim's bank, saying 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 is persuaded by the suspect 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.
- Victim receives a message (either email or through social media) from someone purporting to be a friend of theirs. The suspect uses the outbreak as a reason for requiring financial assistance. The victim transfers money to the suspect, believing it to be their friend.
- Suspect advertises a pet online (puppy or kitten) and uses the outbreak as a reason the victim can't come and see the animal. The suspect sends photos and persuades the victim to make payment in advance. The suspect never provides the pet.
- Victim receives a call with an automated message purporting to be from the government, stating that all individuals now need to wear a face mask when they leave their residence. The message tells the victim to press 1 in order to purchase a mask.

New trends

- We are now monitoring the number of courier frauds which have occurred during lockdown. This currently stands at 129 with losses of £356,499. To help in getting protect messaging out, we have uploaded a number of social media assets to the resources section of the Action Fraud website for people to utilise.

- The highest loss in the last 24 hours was for £11,980 which related to a push payment fraud. Initially, the victim received a text message, purporting to be from HMRC, with a link which they clicked on. This led them to a form which they completed. The victim then received another text message purporting to be from their bank, Barclays, instructing them to call and providing a number. The victim called this number but received an automated message that said the lines were busy due to COVID-19 and the bank's fraud team would call them back. The victim then received a call that appeared on their phone as from Barclays, and were informed their bank account had been compromised and the Barclays Fraud Team had set up a secure account for the victim to transfer their money into. Another report with an almost identical MO resulted in the victim losing £2,098.

Phishing/smishing

Smishing texts spoofing HMRC:-

Text messages are being sent to recipients, purporting to be from HMRC, advising they can get a tax refund of up to £400. This text features a link to a fake government website where the recipient can determine whether they are eligible for a refund.

NOTE: Action Fraud has issued an alert on these scams on our website and digital channels.

Free Tesco vouchers:-

Phishing emails are being sent to recipients claiming to be from Tesco, offering free vouchers. The email features a link for recipients to register and claim their free voucher which provides an opportunity for criminals to steal email logins, passwords and personal details.

NOTE: Action Fraud has issued an alert on these scams on our website and digital channels.

COVID-19 Government grants:-

Phishing attempts claiming to be from the UK Business Advice Bureau, offering government grants up to £25,000, aimed at small businesses. There is a telephone number, email address, and business address, provided to the recipient if they would like to proceed or require further information.

World Health Organization (WHO) emails:-

Emails purporting to be from the World Health Organization (WHO) are informing recipients that they have been selected to receive a grant of $15,000 due to the outbreak. A follow-up email address is provided for recipients to seek further details.

A similar hook is being used by criminals claiming to be from the WHO Reward Department and informing recipients they have been chosen to receive a compensation payment of $500,000 due to the outbreak. Recipients are asked to contact the payment department and provide their personal details to progress the payment.

COVID-19 rapid self-testing kit emails:-

We have received a small number of reports regarding a phishing email claiming to be sent from Clarity Medical Healthcare, selling COVID-19 rapid self-testing kits as a result of government announcements on testing. These emails provide a website address where recipients can make pre-orders.

Virgin Media emails:-

We've been receiving reports of emails purporting to be from Virgin Media, informing recipients that their bill is ready to view. The emails include information on how Virgin Media are responding to the COVID-19 outbreak. The bill amount commonly equates to £60.78.

We've also seen emails purporting to be from the Virgin Media e-billing team, advising the recipient that their account will be frozen because their bank details couldn't be validated. These emails make reference to the lockdown period. They use the Virgin Media logo and are personalised with the recipient's email address. Recipients are asked to click on a link to re-validate and amend their billing details. The link provides an opportunity for fraudsters to steal email passwords and personal details.

In addition, fraudsters are sending emails including:-

- 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;
- Directing recipients to a coronavirus map so they can monitor the situation. When recipients click on the link provided, they are asked to download a "live map" to allow them to track the number of cases for a specific country or globally, overall. This download provides an opportunity for criminals to infect devices with malware and attempt to gain unauthorised access to a network.

REMEMBER:

Detailed counter fraud advice is available online, including from Scamsmart, CIFAS, TakeFive, Citizens Advice, Trading Standards and the National Cyber Security Centre. There is bespoke advice about COVID-19 fraud on the Action Fraud website.

Reporting to Action Fraud can be done online at https://www.actionfraud.police.uk or by calling 0300 123 2040. If you live in Scotland, please report directly to Police Scotland by calling 101. For up-to-date information on COVID-19 fraud please follow Action Fraud on Twitter.

Forward suspicious emails claiming to be from HMRC to phishing@hmrc.gov.uk and texts to 60599. Check HMRC-related phishing, or bogus, emails or text messages against examples published on GOV.UK.