Coronavirus scams

## **Be alert to coronavirus scams**

It’s always important to be aware of scams but now more than ever you need to be alert as you may find you’re seeing more of them as the situation with the coronavirus continues worldwide.

## **How to avoid scams**

To avoid scams

* don’t click on links or open attachments in emails and text messages unless you’re sure they’re from a legitimate source - scammers will go to great lengths to make their communications with you look genuine.
* you shouldn’t ever give out personal or financial information over the phone
* only purchase goods online from trusted and legitimate retailers and, if you have one, use a credit card as this will offer you greater insurance.
* don’t be rushed into making a decision. If it sounds too good to be true it probably is.
* don’t assume everyone is genuine. It’s okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
* don’t let anyone into your home without verifying their identity and checking they have official documentation or ID card.
* if someone claims to represent a charity, ask them for ID. Be suspicious of requests for money up front. If someone attempts to pressurise you into accepting a service they are unlikely to be genuine. Check with family and friends before accepting offers of help if you are unsure.

## **Report scams**

If you have been the victim of an online scam or rip-off, you can get advice or book a face-to-face appointment with a Citizens Advice Scams Action adviser by calling: 0808 250 5050

To report a scam call Police on 101.

Contact your bank if you think you have been scammed.

## **Current scams to look out for**

To learn more about the different types of scams visit [Friends Against Scams](http://www.friendsagainstscams.org.uk/).

Below are some of the known scams to look out for.

### **HMRC tax refund**

Messages and emails claiming to be from HMRC offering a tax refund due to changes in the law around Covid-19, you’re asked to click a link which takes you to a fraudulent website. If you receive a message like this, delete it immediately and do not click any of the links it contains.

### **Center for Disease Control or World Health Organisation**

Messages and emails claiming to be from the Center for Disease Control or the World Health Organisation offer you the chance to view a list of confirmed cases within your local area by clicking on a link or making a Bitcoin payment. These are a scam, delete them immediately and do not click on any of the links.

### **Virologist advice**

Messages claiming to be from a virologist sending an attached document with instructions on how to avoid the Coronavirus. The attachment is malicious and should not be opened. Delete them immediately.

### **Online sales of face masks and hand sanitiser**

Fraudulent online sales of masks and hand sanitiser which never materialise. If an online shopping offer looks too good to be true, then it probably is. We’ve heard of shoppers being asked to send a direct payment, avoiding the use of secure payment facilities such as PayPal. The money is then unable to be returned when the buyer doesn’t receive the products

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. If you decide to go ahead with the purchase, use a credit card if you have one, as most major credit card providers insure online purchases.

### **Insurance or medical plans claiming to have a Coronavirus cure**

Phone calls telling you that there are insurance plans or medical plans which will give you a cure to the Coronavirus / COVID19. These are a scam. Hang up the phone and do not engage with the caller.

### **Microsoft / BT notifications of a computer virus**

Phone calls telling you that your laptop or network has a virus and that fraudsters are accessing your data. If you get calls like this, hang up and do not engage with the caller.

### **Unsolicited visitors offering free Coronavirus testing**

Individuals are visiting people’s homes and offering free Coronavirus testing. Do not open your door to anyone that you don’t know and if they claim to be from a legitimate organisation, ask to see their ID before you even think about engaging with them.

### **Pension scams**

The Financial Conduct Authority have [guidance on how to look out for and avoid pension scams](https://www.fca.org.uk/scamsmart/how-avoid-pension-scams).