



As joint enforcers of The Health Protection (Coronavirus) (Restrictions) (Scotland) Regulations 2020, our team has been very busy ensuring that only businesses permitted to do so are open and providing advice to businesses to enable them to operate safely.

Scams latest

Scams have been on the increase, some specifically related to coronavirus. Below are a few of the more common current scams with links to the Trading Standards Scotland website for more details.



Telephone scams

- Cold calls trying to sell you [insurance or a new warranty](#) for various appliances, including white goods, televisions and solar panels
- [Various calls purportedly from HMRC](#) saying that you have committed tax fraud and that a warrant has been issued for your arrest or that you are [due a tax rebate](#) and asking you for personal and bank details
- Cold calls purportedly from Microsoft or your [broadband provider](#) asking for remote access to your computer or saying that your service will be cut off unless you pay a fee
- Automated calls purportedly [from your bank](#) saying that a payment has been sent overseas from your account - you are asked to press 1 to speak to an advisor
- Cold calls carrying out a health survey or offering to arrange a home visit [to sell mobility aids](#)
- [Misleading energy marketing calls](#) advertising grants for energy saving devices, trying to sell warranties for solar panels or carrying out surveys about double glazing.

Avoiding phone scams

- Do not press 1 or follow any other instruction given in an automated message
- If you are speaking to a person, don't give them any personal information, don't agree to make any payments and never allow them to access your computer remotely
- Contact your bank immediately if you think you may have made a payment to a scammer or if you are worried that a fraudulent transaction has been made from your account. Use the phone number on your bank statement or a publicly listed number (don't use a number given to you by a cold caller). To ensure that you are disconnected from the cold caller, phone another number such as 123 before phoning your bank or call them from another phone.
- Never agree to make a payment for goods or services on the spot – get at least two other quotes from trusted companies.

Report scam calls to us at trading.standards@east-ayrshire.gov.uk. You can find a trusted trader by visiting www.trustedtrader.scot/EastAyrshire

National Insurance scam

Some of our colleagues have received scam emails this week purporting to be from the UK Government, saying that they have established a 'new tax refund programme for dealing with the coronavirus pandemic'. The official-looking email (with Government logos) goes on to say that, based on your National Insurance contributions, you are eligible for a tax refund. You are asked to click on a link to access your refund.

In April alone, HMRC received over **43,000** complaints about phishing emails. They regularly update their [list of genuine communications](#) to help you avoid scams.

Businesses against scams

Businesses Against Scams has been set up by the National Trading Standards Scams Team and includes a number of resources that companies can share with their employees which can educate them on a variety of common business related frauds such as Government grant and tax rebate scams. Sign up your business at <https://www.friendsagainstscams.org.uk/BAS>





Contact tracing scams

It has been reported that a scam text was sent to a Scottish consumer, saying that a 'COVID Home Testing Team' will visit your home at a specified date and time.

It goes on to say that the team will enter your property and that you will need to wait in a separate room while they put on protective clothing. This is an attempt by fraudsters to gain entry to your home.

We have also been made aware of scam calls linked to NHS Scotland's [Test and Protect](#) service, including cold callers claiming to be from the NHS who try to obtain bank details and payment for testing kits.

If you are suspicious about the identity of a caller, hang up and call your [local NHS switchboard](#). They will be able to verify whether a call is genuine.

Remember that genuine contact tracers will NEVER ask for financial details or payment for goods or services.

Holidays and travel

Have your travel plans been disrupted by Coronavirus? Your rights have not changed if the travel company cancels your holiday.

Under the The Package Travel and Linked Travel Arrangements Regulations 2018, you are entitled to a refund, but the majority of travel companies are offering alternatives, like free changes to alternative dates and vouchers for future holidays. It is your choice, but a refund may take longer to receive.

Don't be tempted to cancel your holiday, you will then be liable for cancellation costs. It is best to wait till the travel company cancels it.

On flights only, if your flight is cancelled you are entitled to a refund as long as your booking is with an EU airline or your flight is from an EU airport. The airline should contact you about the cancellation. They may offer to rebook to a later date at no extra cost, but you can seek a refund.

Further information can be found at www.which.co.uk/news/2020/06/coronavirus-outbreak-advice-for-travellers/

IPTV investigations

Illicit IPTV streaming services are where customers can access premium television without a subscription from the rights holder. With evidence that the use of IPTV is on the rise, our service, in conjunction with Trading Standards Scotland recently carried out an investigation into IPTV services being provided locally through websites and social media.

The investigation uncovered several instances of illicit IPTV services being advertised on social media. This resulted in a website being taken down by the web host and warning letters being sent to two individuals.



Why should you avoid using illicit IPTV services?

Apart from the obvious fact that it is against the law to provide these services, there are other problems.

Downloading content to your device from an unauthorised source runs the risk of viruses and malware being introduced to your hardware.

The services are often unreliable. Paying an upfront subscription may leave you out of pocket if your service is unwatchable due to a poor quality picture or constant buffering. Your service may end up not working at all. Do you think you will have much chance of getting a refund?

Also, legitimate companies will suffer financial loss through the continued by-passing of their subscription services, ultimately leading to a rise in prices. If you are aware of anyone promoting or providing IPTV services, please get in touch.

