**Check what to look for first**

Use the following checklist to decide if the contact you’ve received is a scam. You can use it for phone calls, emails and text messages.

It could be a scam if it:

* is unexpected
* offers a refund, tax rebate or grant
* asks for personal information like bank details
* is threatening
* tells you to transfer money

For more help view [examples of HMRC related phishing emails and bogus contact](https://www.gov.uk/government/publications/phishing-and-bogus-emails-hm-revenue-and-customs-examples).

Check a [list of genuine HMRC contact and campaigns](https://www.gov.uk/government/publications/genuine-hmrc-contact-and-recognising-phishing-emails) to help you decide if the one you’ve received is genuine. Report any suspicious phone calls.

**Other signs to look out for**

**Suspicious phone calls**

You can be sure that HMRC will:

* only ever call you asking about a claim or payment on a debt that you already know about
* never leave a voicemail threatening legal action
* never give the reason for a call on a voice message

**WhatsApp messages**

If you receive any communication through WhatsApp claiming to be from HMRC it’s a scam. Take a screenshot and forward it as an email.

**Gift or payment vouchers**

HMRC will never ask you to pay with gift or payment vouchers.