This is how you can verify you are actually being contacted by the government's Test and Trace service

At the end of May, the government launched its Test and Trace service, aimed at contacting those who may have come into contact with someone with coronavirus symptoms.

To ensure that a contact with you is genuine, here are some things to look out for.

What you will be asked for

Firstly, real contact tracers will never do any of the following:

- Ask you for details of card or bank account numbers
- Ask you to provide or fill in social media login details
- Ask you to set up a pin
- Ask you to download anything

If you are asked for these types of information, you can report the incident to Action Fraud.

You should only be asked for the information found on the contact tracing website and on the gov.uk site.

This will include your full name, date of birth, and details of any symptoms you may have.

How you will be contacted

If you have **tested positive** for coronavirus, you will either receive a call, text, or email from NHS Test and Trace with instructions on how to share details of people you have been in close recent contact with.

If you've **been in contact** with someone who has tested positive, you will be contacted in the same ways and asked about symptoms.

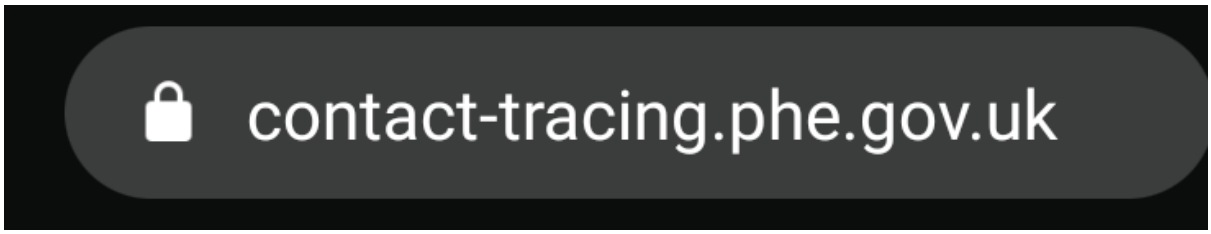
You will only ever be called from the number 0300 013 5000, or you will be texted from "NHS".

However, as some have pointed out on Twitter, it is relatively easy for scammers to fake numbers.

Because of this, **if you do not feel comfortable talking on the phone, or suspect the call to be a scam,** you can ask for an email or a text that will invite you to use the Test and Trace web site instead.

From this email, **you should only ever be directed to this web address**: contact-tracing.phe.gov.uk

You can check this by looking in the address bar near the top of your web browser to see if this is the address shown—it should also have a small padlock symbol next to it, indicating that the website connection is secure.



If you see a different address, it is likely to be a scam, and you should close the window immediately, and report the site to Google. Check carefully—scammers sometimes buy web addresses that look similar to the real address to fool people.

If in any doubt, always submit information via the Test and Trace website. Genuine tracers will be able to provide you with an account ID during the call, or it will be in a text or email sent.

By Rachael Krishna (Full Fact)