HMRC's advice on avoiding cyber and phone scams

Top tip

HM Revenue and Customs (HMRC) is warning people to be careful if they are contacted out of the blue by someone asking for money or personal information. The department sees high numbers of fraudsters emailing, calling or texting people claiming to be from HMRC. If in doubt, HMRC advises people not to reply directly to anything suspicious, but to contact the department straight away and to search GOV.UK for 'HMRC scams'.

Is it a scam?

You can be sure that HMRC won't ring out of the blue threatening your arrest. But if someone contacts you claiming to be from HMRC, it could be a scam. The department will only ever call asking for payment on a tax or tax credit debt that you already know about, usually through a letter (or your Self Assessment tax return).

Tax scam numbers
 In the last year, HMRC:

- received 1,048,396 referrals from the public about suspicious contact, nearly half offering bogus tax 'rebates' or 'refunds'
- worked with the telecoms industry and Ofcom to remove nearly 2,460 phone numbers being used to commit tax phone scams
- received 441,954 reports of phone scams in total, 117% up on the previous year
- reported more than 13,315 malicious web pages for takedown
- detected 462 COVID-19 financial scams, most by text message
- asked internet service providers to take down 441 COVID-19 scam web pages.

Many scams mimic government messages to so that they look authentic and reassuring. HMRC is a familiar brand, which criminals abuse to add credibility to their scams.

The main things to look out for

- Is the contact unexpected?
- Does it offer a refund, rebate or financial support?
- Does it ask for personal information?
- Is it threatening?
- Does it ask you to transfer money?

Criminals are usually trying to steal your money or your personal information to sell on to others. Links or files in emails or texts could also download dangerous software onto your machine or phone. This could gather your personal data, or lock your machine until you pay a ransom.

If you are contacted out of the blue by someone claiming to be from HMRC, by phone, email or text, it is therefore important to ask yourself the questions above before you respond.

If you aren't sure about the identity of a caller, HMRC recommends that you do not speak to them.

HMRC's advice

    Stop:
- Take a moment to think before parting with your money or information.
- Don't give out private information or reply to text messages, and don't download attachments or click on links in texts or emails you weren't expecting.
- Do not trust caller ID on phones. Numbers can be spoofed.

    Challenge:
- It's ok to reject, refuse or ignore any requests - only criminals will try to rush or panic you.
- Search 'scams' on GOV.UK for information on how to recognise genuine HMRC contact and how to avoid and report scams.

Protect:
- Forward suspicious emails claiming to be from HMRC to phishing@hmrc.gov.uk and texts to 60599. Report scam phone calls on GOV.UK.
- Contact your bank immediately if you think you've fallen victim to a scam, and report it to Action Fraud (in Scotland, contact the police on 101).

HMRC's fight against cyber and phone criminals

HMRC prevents scams by:
- automatically spotting most cyber tax scams before the public reports them
- using ground-breaking technologies to prevent misleading and malicious communications ever reaching our citizens
- helping to warn the public by sharing details and examples of genuine and scam communications on GOV.UK
- making it easy for people to report tax scams: at **phishing@hmrc.gov.uk**, **60599** for texts, and using a suspicious phone call reporting form on **GOV.UK**
- tackling misleading websites designed to make people pay for services that should be free or low cost
- working closely with national and international law enforcement organisations
- sharing warnings with media.

Where to find more advice

The National Cyber Security Centre offers a range of helpful advice on how to keep secure online at CyberAware.gov.uk.

Ends