

Self Assessment customers warned about scammers posing as HMRC

Self Assessment customers should be alert to criminals claiming to be from HM Revenue and Customs (HMRC).

As the department issues thousands of SMS messages and emails as part of its annual Self Assessment tax return push, HMRC is warning customers completing their returns to take care to avoid being caught out by scammers. The annual tax return deadline is on 31 January 2021.

The department knows that fraudsters use calls, emails or texts to contact customers. In the last 12 months, HMRC has responded to more than 846,000 referrals of suspicious HMRC contact from the public, and reported over 15,500 malicious web pages to internet service providers to be taken down. Almost 500,000 of the referrals from the public offered bogus tax rebates.

Many scams target customers to inform them of a fake 'tax rebate' or 'tax refund' they are due. The imposters use language intended to convince them to hand over personal information, including bank details, in order to claim the 'refund'. Criminals will use this information to access customers' bank accounts, trick them into paying fictitious tax bills, or sell on their personal information to other criminals.

HMRC's Interim Director General for Customer Services, Karl Khan, said:

We know that criminals take advantage of the Self Assessment deadline to panic customers into sharing their personal or financial details and even paying bogus 'tax due'.

If someone calls, emails or texts claiming to be from HMRC, offering financial help or asking for money, it might be a scam. Please take a moment to think before parting with any private information or money.

Pauline Smith, Head of [Action Fraud](#), said:

Criminals are experts at impersonating organisations that we know and trust. We work closely with HMRC to raise awareness of current scams and encourage people to report any suspicious calls or messages they receive, even if they haven't acted on them, to the relevant channels.

This information is crucial in disrupting criminal activity and is already helping HMRC take down fraudulent websites being used to facilitate fraud.

It's important to remember if you're contacted out the blue by someone purporting to be from HMRC asking for your personal or financial details, or offering you a tax rebate, grant or refund, this could be a scam.

Do not respond, hang up the phone, and take care not to click on any links in unexpected emails or text messages. You should contact HMRC directly using a phone number you've used before to check if the communication you have received is genuine.

If you've been the victim of fraud, contact your bank immediately and please [report it to Action Fraud online](#) or by calling 0300 123 2040.

HMRC is also warning the public to be aware of websites that charge for government services – such as call connection sites – that are in fact free or charged at local call rates. Other companies charge people for help getting 'tax refunds'. One way to safely claim a tax refund for free is to log into your [Personal Tax Account](#).

HMRC has a dedicated Customer Protection team that identifies and closes down scams but asks the public to recognise the signs to avoid becoming a victim. HMRC regularly publishes examples of new scams on GOV.UK to help customers recognise phishing emails and bogus contact by email, text or phone.

Ways to spot a tax scam

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

Self Assessment customers can complete their tax return online and [help and support](#) is available on GOV.UK.

To protect against identity fraud customers must verify their identity when accessing HMRC's online services. They must have two sources of information including:

- credit reference agency data
- tax credits
- P60/payslip
- UK Passport

Further information

In the 12 months to October 2020, HMRC:

- responded to 846,435 referrals of suspicious HMRC contact from the public. More than 495,937 of these offered bogus tax rebates
- responded to 306,219 reports of phone scams, an increase of 47% on the previous 12 months. In October 2020, HMRC received reports of 44,543 phone scams
- worked with the telecoms industry and Ofcom to remove more than 3,387 phone numbers being used to perpetrate HMRC-related phone scams
- reported 15,518 malicious web pages to internet service providers to be taken down

If you're concerned about falling victim to a potential scam, remember:

Stop:

- take a moment to think before parting with your information or money
- 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

Challenge:

- it's ok to reject, refuse or ignore any requests – only criminals will try to rush or panic you
- read about [avoiding scams](#) on GOV.UK: information on how to recognise genuine HMRC contact and avoid and report scams

Protect:

- forward suspicious emails claiming to be from HMRC to phishing@hmrc.gov.uk and texts to 60599.
- contact your bank immediately if you think you've fallen victim to a scam, and report it to [Action Fraud](#)