

Tax Fraud

It's that time of year when businesses submit their Tax and request rebates. Fraudsters will tailor their scams to these annual procedures to manipulate you into paying a penalty; alternatively, they might entice you into a rebate to get your personal and financial information.

HMRC will never request a penalty payment or offer a Tax refund through any form of electronic communication.

Take a minute and pause when receiving any email, text or call and question the request/offer.

To identify fraudulent Tax requests

- Look for a sense of urgency, threat or enticement/offer.
- Hover over the link to reveal the true website path. The reputable website is <https://www.gov.uk> anything different to this is a scam. To trick you into thinking it's the "real deal", they might make small changes such as [gov.co.uk](https://www.gov.co.uk), [gov.org](https://www.gov.org), [gov.com](https://www.gov.com), [g0v.uk](https://www.g0v.uk) for example.
- Check if the email/text is generic. It might say "Dear Customer" or not address anyone at all.
- Lookout for spelling and grammatical errors.
- Examine the quality of the logo, a fake email is likely to use a low-quality image.
- Check whether the body of the email is contained within an image. This might contain malware or have a malicious link embedded.
- Check the sender email address. At first glance it might look to be from the Government but after investigation you can reveal it is not a genuine sender.
- Call and double check the request if you have any concerns. You can find genuine contact information here: <https://www.gov.uk/contact>
- Question a caller to confirm they are who they claim to be. Keep in mind, prolonged conversation to the fraudster can cost money.

Actions if you think it's a scam

- Hang up the phone and call HMRC on a genuine number: <https://www.gov.uk/contact>
- Never open an attachment from an unexpected source as it can contain malware. Scan all attachments with AntiVirus/AntiMalware tools.
- Don't click the link. If you do click the link don't panic but report it to your line manager.
- Report fraudulent emails, texts and calls to:
 - HMRC: <https://www.gov.uk/government/organisations/hm-revenue-customs/contact/reporting-fraudulent-emails>
And <https://www.gov.uk/report-suspicious-emails-websites-phishing/report-hmrc-phishing-emails-texts-and-phone-call-scams>
 - Forward an email to the NCSC reporting email: report@phishing.gov.uk.
 - If you fall victim to these scams report to Action Fraud: <https://www.actionfraud.police.uk/>
- After reporting and following internal procedures, delete the fake emails and texts and block fraudulent numbers.

For examples of these scams, visit the Government website:
<https://www.gov.uk/government/publications/phishing-and-bogus-emails-hm-revenue-and-customs-examples/phishing-emails-and-bogus-contact-hm-revenue-and-customs-examples>

Genuine communication from HMRC can be found here:
<https://www.gov.uk/guidance/check-a-list-of-genuine-hmrc-contacts>