Press release: HMRC warns on tax refund scams

HMRC is calling on people to stay vigilant in the fight against fraudsters, who are using email and text messages to scam them out of their savings.

The tax authority is currently processing tax refunds after the end of the 2017 to 2018 tax year. However, criminals are taking advantage of this by sending out scam emails and SMS-messages to trick the public into thinking they have received a tax rebate so they hand over their account and personal details.

Treasury Minister Mel Stride MP, the Financial Secretary to the Treasury, said:

> HMRC only informs you about tax refunds through the post or through your pay via your employer. All emails, text messages, or voicemail messages saying you have a tax refund are a scam. Do not click on any links in these messages, and forward them to HMRC's phishing email address and phone number.
>
> We know that criminals will try and use events like the end of the financial year, the self-assessment deadline, and the issuing of tax refunds to target the public and attempt to get them to reveal their personal data. It is important to be alert to the danger.

Many of these fraudulent emails and texts include links which take the user to dubious websites where their information can be stolen. These sites are a focus of HMRC's efforts to tackle fraud. In March 2018, it requested 2,672 phishing websites be taken down and received 84,549 phishing reports. This kind of phishing is expected to continue in the coming months as genuine tax refunds are issued.

Income Tax for 6 April 2017 to 5 April 2018 will be calculated over the coming months and anyone owed a genuine tax rebate will receive a tax calculation letter by post between June and October.

If you haven't paid the right amount at the end of the tax year, HMRC will post you a tax calculation. This can be a P800 or a Simple Assessment letter. If you have paid too much tax, the letter will explain how you can get your refund paid to you. If you have not paid enough tax, the letter will tell you how much you owe and how you can pay.

HMRC advice

HMRC advises customers to:

- recognise the signs – genuine organisations like banks and HMRC will never contact you out of the blue to ask for your PIN, password or bank details
- stay safe – do not give out private information, reply to text messages, download attachments or click on links in emails you weren't expecting
- take action – forward suspicious emails claiming to be from HMRC to phishing@hmrc.gsi.gov.uk and texts to 60599, or contact Action Fraud on 0300 123 2040 to report any suspicious calls or use its online fraud reporting tool
- check GOV.UK for information on how to avoid and report scams and recognise genuine HMRC contact
- if you think you have received an HMRC-related phishing/bogus email or text message, you can check it against the examples shown in this guide

HMRC action

HMRC has taken a range of action to protect the public from scams, including:

- from April 2017 to March 2018, reported 14,631 malicious websites for takedown
- from April 2017 to March 2018, received 771,227 customer phishing email/SMS referrals
- from April 2017 to March 2018, received 1.1 million direct visits to HMRC security pages on GOV.UK
- implemented SMS firewalling – working with industry to deliver a pilot to reduce SMS abuse, resulting in a 90% decrease in reported abuse of protected HMRC SMS tags