

PART ONE

PHISHING SCAMS.

Phishing is an attempt to obtain sensitive personal information by pretending to be a legitimate organisation (like HMRC) in communications such as phone calls, texts and emails. Whilst many phishing scams can be easy to spot, others are quite sophisticated and can look like genuine HMRC communications.

HOW TO SPOT PHISHING

A key feature of phishing scams is that they will ask you to provide personal or financial details (such as bank or credit card details) in order to, for example, receive a tax refund. HMRC stress that they will never use texts or emails to:

- Ask for personal or payment information.
- Inform you of a tax rebate or penalty.

GENERAL POINTERS

Indications that a communication is fraudulent include:

- Poor grammar and spelling mistakes.
- Incorrect sender addresses: these may be similar to, but not the same as, legitimate HMRC email addresses.
- The use of a generic greeting such as Dear Customer.
- Links to bogus websites: these may look very similar to the HMRC website but often contain links to other websites or requests to input large amounts of personal information.

GENUINE HMRC EMAILS

- Address you using the name you've provided to HMRC (usually when signing up for HMRC online services).
- Always include information on how to reporting phishing emails.
- Never give a direct personal email address to reply to (unless you are aware this is a genuine HMRC advisor).
- Never provide a link to a log-in page or a form asking for information: instead you will be asked to log into your online account through the normal channels.

HMRC publish up to date lists of genuine topical HMRC calls, letters and digital communications which can be referred to if you are in doubt.



PART TWO

PHISHING SCAMS.

HMRC publish up to date lists of genuine topical HMRC calls, letters and digital communications which can be referred to if you are in doubt.

REPORTING SUSPICIOUS HMRC COMMUNICATIONS

Online:

[Click here to use the online form](#) to tell HMRC if you've received a phone call you do not think is genuine. You'll need to give your email address.

Email:

Forward details of suspicious emails to HMRC's phishing team:

phishing@hmrc.gov.uk

You should give details of what you're reporting in the subject line (for example 'Suspicious email address'). HMRC will never send notifications of a tax rebate or ask you to disclose personal or payment information by email.

Suspicious Text Messages:

Forward suspicious text messages to 60599. Text messages will be charged at your network rate. HMRC will never send notifications of a tax rebate or ask you to disclose personal or payment information by text message.

The logo consists of the letters 'C' and 'S' in a bold, green, sans-serif font. The 'C' is on the left and the 'S' is on the right, both rendered in a light green color.