



HMRC Alert

What you need to know

- Action Fraud has experienced an increase in the reporting of malicious calls and voicemails, to members of the public purporting to be from Her Majesty's Revenue & Customs (HMRC).
- Fraudsters are spoofing genuine HMRC telephone numbers to deceive their victims over the phone. The fraudsters state that as a result of the victim's non-payment of tax or other duty, the victim is liable for prosecution or other legal proceedings in order to settle the balance. The fraudsters suggest victims can avoid this, by arranging payment to be made immediately by methods such as bank transfer or by purchasing iTunes gift cards.
- If the victim is hesitant or refuses to comply, the suspect makes a threat such as immediate arrest, sending bailiffs to the victim's address or, in some cases, deportation.
- Often, the period for which the tax is allegedly due is distant enough to guarantee the victim will have little, if any, paperwork or ability to verify the claims. Once the money is paid the suspects sever all contact with the victim.
- In genuine cases, HMRC will initially make direct contact with you via post/letter and potentially follow up that letter with a phone call at a later date.
- If HMRC contact you via telephone they will quote the reference number on the initial letter you should have received. HMRC will not discuss something you are not already aware of, like a tax investigation, and will **NOT** demand immediate payment.

It is vital that the public exercise caution when receiving messages or telephone calls of this nature.

What you need to do

- Always question unsolicited requests for your personal or financial information. Just because someone knows your basic details (such as your name and contact details), it doesn't mean they are genuine. Instead, contact the company directly using trusted methods such as a known email address or phone number.
- Legitimate organisations wouldn't ask you to pay taxes, bills or fees using an iTunes gift card, or any other type of voucher. If you're contacted by anyone that asks you to do this, you're likely the target of a scam
- Don't be rushed or pressured into making a decision. Under no circumstances would a genuine bank or some other trusted organisation force you to make a financial transaction on the spot.
- Report Phishing attempts. If you receive a call, text or email of this nature and have not lost money, you can report this as phishing to Action Fraud