

## General advice about scams and how to avoid them

Major warning signs are when someone:

- asks for your bank account/credit card details
- asks for your credit/debit card and offers to go and withdraw the money for you
- offers to drive you to the bank/post office so that you can withdraw the money.

**E-mail scams** usually feature:

- a request for money to help someone release money following a bereavement and a promise to reward you with a huge sum of money for your help
- a warning that your 'account' (e-mail, bank, membership etc) is about to be closed unless you verify your details
- a message which is only accessed by clicking on a link

These scams involve so-called '**phishing**' – obtaining personal or financial details by stealth. This is usually achieved by asking you to 'log-in' to your account, thereby disclosing your password. The clue that an e-mail message is a scam is in the text of the message; which often includes poor grammar and spelling errors. These scams are best avoided by not opening any e-mail from an unknown sender and, if you do, by not clicking on any of the links in the message and by not opening any attachments.

Other ways of obtaining your data involves bogus websites, which look like official websites eg HMRC, Home Office, Microsoft™.

If you are not sure about the **origin of an e-mail message**, hover the cursor over the sender's address and the real e-mail address will be revealed.

**Please report the 'phishing scam'** by clicking on the 'not junk' tab at the top of the page and using the drop-down menu.

**Note:** The Vantage Motor Group has recently published a [guide](#) 'to protect care buyers from dodgy dealers and common car scams', which can also be found on the company's blog.