

How to spot a scam?

Keep this simple four-step reminder somewhere visible, such as next to your phone or on the fridge. If any of these apply, stop and think before you act.



Secrecy

You are told to keep it a secret or that the offer is “too good to miss”. If you must lie to the bank about the nature of a money transaction, not tell the cashier you’re buying gift cards after someone called you, not tell your family about the issue or even tick to say you’re transferring money to friends on PayPal when it’s not a friend, it’s almost certainly a scam.



Contact

(Out of the blue)

The message, call, or email is unexpected. Scams often begin with a message or call ‘out of the blue’, be it by e-mail, text message, phone call, a pop-up message on your computer or something similar.



Action

(Now)

You are pressured to respond immediately. A fraudster will try to rush you into doing something because they don’t want to give you the time to think or possibly tell a friend who might suggest it’s a scam. They may appeal to your honest nature to right a wrong (e.g. you received too much money for a refund.)



Money

You are asked for payment, passwords, or codes. Be very wary anytime you’re making a payment or sharing card details, as most scams are about getting money.

Share these tips with friends and family who might be less confident online.

Top Tip

Think about setting up a secret word between family members that no one outside your close circle knows. This way, if you receive any messages starting, “Hi Mum, I’ve lost my phone and need help,” you can say: “OK. What’s the secret word?” If they don’t know it, it’s not them and most likely a scam.

thinkbroadband[®]