



VISHING ALERT

Received a call purporting to be from Amazon, BT, UK HMRC, bank or other organisation you weren't expecting?

IT COULD WELL BE A FRAUDSTER ON THE OTHER END OF THE LINE!



WHAT TO LOOK OUT FOR

Many begin with an automated voice requesting that the call recipient presses '1' before being redirected to a scam operator. They will often create a sense of urgency or threaten negative action as a result of not following their instructions.

THEIR INTENTIONS

These scammers may aim to gain access to your computer or device remotely and transfer sums of money from your bank into accounts under their control. They may even convince you to transfer money to them.

WHAT TO DO

If ever in doubt about a call, hang up and contact the genuine business using known contact details from an official source.

If possible, use a different phone or wait at least 10 minutes before making a call.



IF YOU BELIEVE MONEY HAS BEEN TRANSFERRED TO A SCAMMER, CONTACT YOUR BANK AS SOON AS POSSIBLE.

IF THE SCAMMERS HAVE ACCESSED YOUR COMPUTER OR DEVICE, TURN IT OFF AND ARRANGE FOR IT TO BE RESTORED BY A COMPETENT IT PROFESSIONAL.



REMAIN VIGILANT AND SHARE THIS ADVICE WITH YOUR FRIENDS, FAMILY AND COLLEAGUES.