LLOYDS

The seven words that reveal you're talking to a scammer: 'Move your money to a safe account'

- **Victims lost £3,516 on average to impersonation scams over the past year, up 10%**
- **Overall impersonation scam cases fell slightly, but bank, police, HMRC, telecoms and Amazon impersonation scams all increased**
- **One victim lost £188,000 to a police impersonation scam**
- **Lloyds shares the simple tips to help people spot a scammer**

Scammers posing as trusted organisations are taking more money from victims, even as the total number of impersonation scam cases has edged down.

New Lloyds data[1] shows victims lost £3,516 on average to impersonation scams over the past year, up 10% on the year before.

Overall cases reported to Lloyds fell by 3%, but fraudsters pretending to be banks, the police, HMRC, broadband and mobile providers and Amazon, all went up.

Impersonation scams, reported to Lloyds 1st July 2024 to 30th June 2025 vs 1st July 2025 to 30th June 2026	
HMRC	+63%
Broadband or mobile provider	+57%
Solicitor	+35%
Amazon	+27%
Police or Bank	+4%
All impersonation scams	**-3%**

More recently, bank and police impersonation scams saw a sharper jump, up +18% jump in the second quarter of 2026, compared with the same period in 2025.

Liz Ziegler, Fraud Prevention Director at Lloyds, said "Summer can be an expensive time of year, with many people focused on managing their finances around holidays, family days out and other seasonal costs. Fraudsters know money is often at the top of peoples' minds and use convincing stories about account issues, refunds or urgent payments to pressure people into acting quickly.

"Remember, your bank or the police will never ask you to move money and, if you hear the words 'safe account', it's a scam. If you're contacted unexpectedly, real organisations will always give you time to check things are genuine."

What is an impersonation scam? How fraudsters make fake messages feel real

Impersonation scams often begin with a phone call, text, email or social media message that looks genuine.

In **police and bank scams**, victims are told their money is at risk and asked to move it to a so-called 'safe account'. In some cases, criminals tell victims their own bank is involved in fraud, then coach them to lie if a genuine bank worker asks why they are moving money.

HMRC scams typically entice people with messages about tax refunds to persuade people to click a link and enter personal or financial details. Victims of HMRC impersonation scams lost £2,288 on average over the past year.

Broadband and mobile provider scams involve claims of issues with a bill, contract or internet connection, before asking for personal details or payment. The average amount lost to broadband and mobile provider impersonation scams was £1,169.

Victims of **Amazon impersonation scams** lost £1,180 on average, most commonly to messages that encourage people to click on links and enter personal details, to release a fictitious package.

Liz Ziegler continued "A scam message is designed to rush you. It will make you feel you need to act straight away or keep things secret. Genuine businesses and organisations will never ask you to lie or keep things to yourself - anyone who asks you to do so is a fraudster."

Top tips from Liz to spot a scammer

- **Never move money to a 'safe account'.** Banks and the police will never ask you to transfer money to protect it from fraud.
- **Never give items to couriers or post them.** Banks and the police will never ask you to hand over cards and PINs, cash or buy expensive items such as gold or jewellery.
- **Don't trust unexpected messages.** Use contact information from official websites, bank cards or genuine correspondence.
- **Never share security codes or passwords.** A genuine organisation will never ask for your full password, PIN or one-time security code.
- **Be truthful.** Criminals tell victims to hide the real reason they're moving money. Your bank's fraud checks are there to protect you, so always be honest about where your money is going and why.
- **Be wary of unexpected tax refund messages.** HMRC does not notify customers of refunds by text message or ask for personal details through links in messages.
- **Hang up and call back.** If you're unsure about a phone call claiming to be from your bank, police or another organisation, end the call and contact the organisation directly using a trusted number.

Case Study
This is a real-life example of an impersonation scam that was reported to Lloyds. The name has been changed to protect the identity of the victim.

Helen's story, aged 85

Helen received a call from someone claiming to be the police. They told Helen they had arrested someone who had cloned her card and was purchasing expensive items in another area of the UK.

She was told to not contact her bank or talk to anyone as this could cause issues with the investigation.

Helen was persuaded to purchase gold bars from a jeweller, having been told there was evidence on the gold which would help support the investigation. The 'police officer' on the phone told her the funds she was using to purchase the gold were not hers, as her money was being held and insured by the police.

The gold was then collected by someone she believed to be an undercover police officer.

She made eight purchases of gold across a five-month period, with a total loss of £188,000.

ENDS

Notes to Eds

Methodology: [1]All figures based on analysis of relevant scams reported by Lloyds Banking Group customers 1st July 2024 to 30th June 2025 vs 1st July 2025 to 30th June 2026

Further advice on spotting HMRC scams

- Never let yourself be rushed. If you receive an unexpected call or message claiming to be from HMRC, always take time to stop and think if the request is genuine before sharing personal information. Genuine HMRC contact details and advice on spotting scams can be found on GOV.UK.
- Report messages claiming to be from HMRC by forwarding texts to 60599 and emails or letters to phishing@hmrc.gov.uk. You can also report phone calls on GOV.UK. This helps stop criminals and protect others from being targeted.