

Report Fraud

Report Fraud alert: Police forces being impersonated in scam calls using 'spoofed' phone numbers

Report Fraud, run by the City of London Police, is urging the public to be sure of who they are talking to following a spike in reports of calls from 'spoofed' police force phone numbers.



Police forces impersonated in scam calls using 'spoofed' phone numbers

The police will never call asking you to transfer money, or share your personal and financial details.

To receive these alerts by email, sign up for free at: reportfraudalert.co.uk

POLICE ALERT

Report Fraud Call 0300 123 2040 reportfraud.police.uk

Find out more: reportfraud.police.uk

Analysis of data from Report Fraud, the national cyber crime and fraud reporting service, shows that there has been an increase in reports made where the caller has purported to be from a police force from a variety of areas across the country. The City of London Police itself, the National Lead Force for fraud, has also taken thousands of crime reports of a similar nature.

But in reality, it is a criminal contacting a member of the public, using a 'spoofed' phone number to try and obtain sensitive personal or financial details so that fraud can then go on to be committed. Often, the criminals will claim that the victim will be helping with an investigation by providing the personal or financial information they are asking for.

While a number of calls about this type of fraud has been made to Report Fraud, this is likely to be the tip of the iceberg and a far bigger problem that is not reported, so the full scale is unknown.

Criminals use 'spoofing' software to intentionally cover up their real caller ID and instead, mirror the phone number of a legitimate organisation. They do this to make it appear that calls or text messages are coming from a trusted organisation like the police, banks or government agencies.

These scam calls may use AI technology, be automated or from a real person. Their main goal is to trick you into sharing personal information or to transfer money.

How to protect yourself

Remember that genuine service providers, banks and the police will NEVER call asking you to transfer money, share personal financial details or hand over remote control of your computer.

If you are in any way suspicious, or feel pressured into anything, hang up and take time to check if the call is genuine. Call back on a number you know to be genuine, for example as shown on your utility bills or the back of your card. You can also call 159 to get through to your bank, or 101 for the police.

Don't trust the Caller ID display on your phone – it's not proof of ID,

Report a suspicious phone call

If you've lost money or have been hacked as a result of responding to a phishing message or scam call, you should report it to Report Fraud.

In England, Wales or Northern Ireland, visit <https://www.reportfraud.police.uk/> or call 0300 123 2040. In Scotland, report to Police Scotland by calling 101.

You should also report suspected scam calls by sending a text to 7726 with the word 'Call' and the caller's number.

If you've shared personal information with a suspicious caller

Learn how to protect yourself [if you think you've shared personal information.](#)

If you've visited a website you think is suspicious, you can [report a scam website](#) or link to us.

Message Sent By

Report Fraud