POLICE SCOTLAND
POILEAS ALBA

Suspicious about a phone call from your “bank”?

Bogus callers can make contact with you by phone and claim to be from your bank or other trusted organisation.

A fraudster may advise you that there has been suspicious activity on your bank account and request you transfer all of your money into a 'safe account'. They may instruct you to hang up the phone and call a number provided by them. However, the fraudster will keep the line open, pretend to be a bank official and provide you with details of the 'safe account' and induce you to carry out the transfer of money in their account. Fraudsters are cunning, creative and often very convincing.

However, your bank will never:

- Phone and ask you for your PIN or full banking password (even by tapping it into the phone keypad)
- Request you to transfer money to another account
- Ask you to withdraw money to hand over to them for safe-keeping
- Send a courier to your home to collect your money, bank cards, PIN or cheque book.

Remember:

- If requested to provide personal or financial information, take time to think about it and remain calm
- If in doubt, just hang up and never give out personal or financial information if you are unsure who you are dealing with and contact your bank on their official phone number
- Fraudsters can make telephone numbers used to call you seem genuine, so don’t rely on this as verification
- Call 101 to report any suspicious activity. If you feel scared or threatened call 999 and ask for the police.

Check our website for more information, tips and advice from us and our partners: ☞
https://www.scotland.police.uk/keep-safe/personal-safety/doorstep-crime-and-bogus-callers

Advice and information on bank scams and frauds can also be found on Trading Standards Scotland (Scam Share) link:

https://www.tsscot.co.uk/bank-scams/

- Do not press 1 or follow any other instructions given in an automated message.

- If you are speaking to a person, don't give them any personal information or bank details, even if they seem to know some of your details already
- Don't click on any buttons or links in unsolicited emails, even if they look official
- Contact your bank immediately if you think you may have made a payment to a scammer or if you are worried that a fraudulent transaction has been made from your account. Use the phone number on your bank statement or a publicly listed number (don't use a number given to you by a cold caller). To ensure that you are disconnected from the cold caller, phone another number such as 123 before phoning your bank or call them from another phone
- **Report bank scams to Advice Direct Scotland. You can also report scam emails to the NCSC**
- **If you have been the victim of fraud, report this to Police Scotland on 101**