



Suspicious phone calls

Would you give a stranger your house keys or your wallet? Probably not, because you don't know them. It's the same on the phone – you can't be sure who you are talking to!

Fraudsters phone people pretending to be Bank of Scotland, the police, or companies such as BT, Microsoft or TalkTalk. They do it to get you to send money, let them access your bank account or take control of your device to steal your personal data. **Stop and think – is this call genuine?**

Telephone fraudsters sound convincing and professional. Here are a few tips on how you can protect yourself and tell a genuine phone call from a scam.

Follow these four steps:

1: Do you really know who's calling?

If the call is unexpected, then they might not be who they say they are. If you're not sure, say you'll call back. Always use a trusted number (not the number the caller is using or asks you to use, and don't assume a caller is from Bank of Scotland even if your caller ID says that it is. For Bank of Scotland, use the number on the back of your card. If the caller says they are from the Police you can call back on 101.

2: Is the caller putting pressure on you?

Fraudsters want to create a sense of urgency to force you to make quick decisions. The scammer might also ask you to "keep it quiet" and not tell anyone about the call. Don't trust anyone trying to silence you or hurry you up.

3: Never let a caller trick you into transferring your money

Never transfer money if a caller says you must do this for "security purposes" to a "safe/secure/holding account". Fraudsters might also say they're from Bank of Scotland telling you that you are due a refund, or that you must complete a test transaction. We'll never ask you to do this so hang up the phone!

It's very rare for the Police or Scotland Yard to call people unexpectedly. If they do, they'll never ask you to move your money. And they'll always follow up with a visit from a Police Officer with photo ID and a warrant number.

4: Don't sign in to your computer for a caller

If an unexpected caller claims there is something wrong with your computer or asks you to download something, this is almost certainly a con.

The caller might claim to be from a broadband provider or trusted software company (even the one you use). But unless you asked for this phone call, it is likely to be a fraud.

If a caller asks you to log in to your computer, tell them you'll make your own arrangements and hang up.

Never tell a caller what you can see on your screen or allow anyone remote access (control of your machine) unless it's a company that you called first.

Be very wary if the caller claims they have accidentally sent you money and ask you to send it back. If in doubt, put the phone down.