How to Deal with a Suspicious Phone Call

If someone calls you unexpectedly and starts asking for personal information, account details, passwords, PINs or security codes, don't feel pressured into responding.

Here's What to Say

"I don't give out personal information or account details during an unsolicited phone call. I'll contact the organisation directly using a trusted number."

Then end the call.

Legitimate organisations will understand and support your decision to verify their identity independently.

Be Aware of Spoofed Numbers

Criminals can manipulate the number that appears on your phone. This is known as **number spoofing**.

A call may appear to come from your bank, the police, HMRC, Microsoft, Amazon, or another trusted organisation when it is actually coming from a fraudster.

Never trust a caller simply because you recognise the number displayed on your phone.

Be Aware of Pressure Tactics

Scammers will often try to keep you on the phone. They may create a sense of urgency, claim there is an immediate problem with your bank account, computer or personal information, or attempt to shock and scare you into acting quickly.

They do this to stop you taking time to think, verify what they are saying, contact the organisation yourself, or seek advice from someone you trust.

Common examples include:

- "Your bank account has been compromised."
- "Money is leaving your account right now."
- "Your computer has been hacked."
- "You owe money and must pay immediately."
- "A loved one is in trouble."
- "We're investigating suspicious activity on your account."

The stronger the pressure, the more suspicious you should be.

Protect Yourself

Never give out passwords, PINs or one-time security codes.

Hang up if you are unsure who is calling.

Contact the organisation yourself using a trusted telephone number from its official website, app, bank card or previous correspondence.

Be aware that phone numbers can be spoofed and should not be relied upon as proof of identity.

Review your social media privacy settings regularly. Scammers will obtain information about you, from social media and other online sources, then use it to try and convince you that they are genuine.

Think carefully before sharing any personal information online. Do your really want your CV available for all to see?

Remember Your ABC

Never Assume. Never Believe. ALWAYS CONFIRM.

If you receive an unexpected call asking for information, don't be rushed into making a decision. Take control of the situation, end the call, and then verify the caller independently. Be curious.

Hang Up. Look Up. Call Back.

When you make the call to a trusted and thoroughly verified number, **you are in control of who you are speaking to.**

To quickly contact your bank call **159**

Don't let the caller provide the number you should call back on. Fraudsters may provide a fake number that connects straight back to them or an accomplice.

Always find the contact details yourself and verify them independently using official websites, apps, bank cards, statements or previous correspondence.

Ideally, call back using a different phone. If this is not possible, wait a few minutes before redialling, particularly if using a landline.

Never trust the number. Trust the verification process.

Reply | Share | Rate



Message Sent By
Mick Harrison
(Devon & Cornwall Police, Cyber Protect Officer, Devon & Cornwall)

Your Devon and Cornwall Community Messaging account...

My Local Area | Message Preferences | System Support | Login | Unsubscribe

---

POWERED BY neighbourhood ALERT®

You are receiving this message because you are registered on Devon and Cornwall Community Messaging. Various Information Providers (organisations) are licensed to send messages via this system. This message was sent by Devon and Cornwall Police and Devon and Cornwall Police does not necessarily represent the views of Devon and Cornwall Community Messaging or other Information Providers.

You can review the messages you receive, configure which Information Providers can see your information, or unsubscribe. You can also review our Terms and Conditions and Privacy Policy.

This email communication makes use of a "Clear Image"(gif) to track results of the email campaign. If you wish to turn off this tracking for future emails, you can do so by not downloading the images in the e-mail itself. All links in the body of this email are shortened to allow click through monitoring.

VISAV Limited is the company which built and owns the Neighbourhood Alert platform that powers this system. VISAV's authorised staff can see your data and is registered with the Information Commissioner's Office as the national Data Controller for the entire database. VISAV needs to see your data to manage the system and provide support; it cannot use it for commercial or promotional purposes.