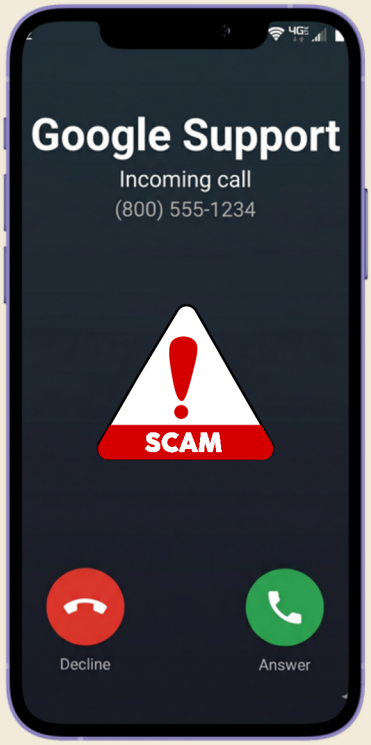
Even if the call sounds real It might still be *a scam*.

AI voice scams now sound **exactly like real humans** on the phone. Robotic delivery, bad accents are no longer reliable warning signs.



01 ANATOMY OF A VOICE SCAM ATTEMPT

- Asks for codes/passwords
- Wants remote access
- Creates urgency/fear
- Pressures you to take action
- Asks you to move money
- Asks you to access a page

If you're not 100% sure, **hang up**

Voice scam losses hit £14.4 billion last year, and the average victim loses between £595 and £13,342 in a single call. The scammers are using perfect-sounding AI bots that you can't tell apart from a real human. If a call seems off, hang up.

02 HOW TO VERIFY IF IT'S A SCAM

Did you initiate the call?
If NO, and the call is about anything sensitive, treat it as a scam.

Hang up. It's not rude to verify
A real representative will never penalise you for hanging up to confirm.

Discard everything the caller gave you.
Caller ID, phone numbers, email addresses, links. All of it is easy to spoof or fabricate.

Find the official contact yourself.
Go directly to the source. Avoid Googling "support number."

Report it, then delete.
Confirm whether the original call was real. If it wasn't, report it to your IT team.

Email: hello@blackswancyber.co.uk
Phone: 01246 927142

BLACK SWAN
CYBER SECURITY SOLUTIONS