

AI voice scam checklist

Before sending money, sharing personal information or acting on an urgent request, please take a moment to run through this checklist.

Verify the caller

- ☐ Have I called the person back using a phone number I already know and trust?
- ☐ Have I spoken to another family member, friend or colleague to confirm the situation?
- ☐ Have I asked a question that only the real person would know the answer to?
- ☐ Have I independently verified the story or situation?
- ☐ If the caller claims to be from a bank, business or government organisation, have I hung up and contacted them directly using an official phone number?

Watch for warning signs

- ☐ Is the caller creating urgency, fear or panic?
- ☐ Are they asking for money, a bank transfer, gift cards or cryptocurrency?
- ☐ Are they asking me to keep the situation secret?
- ☐ Has the caller contacted me from an unfamiliar number and does the request seem unusual?
- ☐ Are they asking me for PINs, codes or passwords?

If in doubt

- ☐ Hang up
- ☐ Verify the request independently
- ☐ Talk to someone you trust
- ☐ Contact your bank immediately if you have shared information or sent money.
- ☐ Does the request seem unusual or out of character for this person?

Family safety tip

Create a family safe word or question.

If a loved one ever calls claiming to be in an emergency, ask for the safe word before taking any action.

Examples:

- What was the name of our first pet?
- What's our family code word?
- Where did we go on holiday last year?

A family member will know the answer. A scammer may not.

Remember

Stop. Check. Protect.

A few extra moments could protect your savings, personal information and peace of mind.

