


Help After a Scam

Being tricked doesn't make you foolish. Scams are designed to deceive.

If something's gone wrong, don't panic. You're not alone, and you *can* take steps to limit the damage. Please read for further information below.

Need support now?

 Call or text **Cyber Shoulder** at **07440 602 591**
...or speak to someone you trust.

We'll listen without judgment and help you take the next step, even if you're unsure what happened. It's always best to ask.

Immediate Actions to Take

1. 🗣️ Tell Someone You Trust

Scammers thrive on silence. Speak to:

- A friend or family member
 - Your bank or building society
 - A trusted organisation like **Cyber Shoulder**
-

2. 🏦 Contact Your Bank (If Money Was Involved)

If you've sent money or given out bank details:

- **Call your bank immediately** — they may be able to stop or recover payments
 - Ask them to **cancel your card** or **freeze your account** if needed
 - Keep a note of who you spoke to and what they said
-

3. 🗝️ Change Any Passwords You Gave Away

If you've shared a password (or use the same one elsewhere):

- **Change it right away** on all affected accounts
- Make it strong: use 3 random words and numbers
- Turn on **two-factor authentication** (2FA) where you can

4. Block the Scammer

Whether it was a message, phone call, or email:

- **Block the number or sender**
 - Don't reply — even to say “stop”
 - Report the message as spam or scam if your device allows
-

5. Report It

Reporting helps stop scams happening to others.

- You can report to **Action Fraud** at 0300 123 2040 or online at actionfraud.police.uk
 - Or call **Cyber Shoulder (07440 602 591)** for guidance. No judgment, just support
-

6. Keep Any Evidence

Save emails, letters, receipts, or screenshots.

They can help your bank or the police investigate what happened.

Remember:

- ☒ Scammers are to blame, not you
 - ☒ Help is always available
 - ☒ Talking about it helps others stay safe too
-