

PRINTABLE GUIDE

Check a suspicious text message

Sender names and displayed numbers can be misleading. Pause and verify unexpected requests using an independent contact route.

Any phone | 2 min read | 5 steps

Before you start

- ☐ The message left unopened where possible
- ☐ A known official contact route for the claimed sender

1. Pause the requested action

Do not reply, call its number or tap its link while checking. Urgency, threats and unexpected payments are reasons to pause. Familiar sender labels and polished branding do not prove authenticity.

- ☐ Done this step

2. Compare it with what you expected

Ask whether you actually placed the order, requested a code or arranged this contact. A message can still be false even when it resembles a real event. Do not give someone a verification code simply because they asked.

- ☐ Done this step

3. Contact the organisation independently

Open its official app, type its known website address or use a number from paperwork you already trust. For a claimed family member, use their existing number. Explain the request without using the text's link as your starting point.

- ☐ Done this step

4. Report through the right route

In the UK, many mobile providers accept suspicious texts forwarded to 7726. Use your message app's forwarding function and follow the provider's reply. Elsewhere, check your provider's reporting route; 7726 is not a universal international service.

☐ Done this step

5. Keep evidence if needed and remove it

Keep useful details privately, then block/report the sender and delete the message if appropriate. If you already shared credentials or payment information, contact the relevant provider through its genuine route promptly and follow its recovery instructions.

☐ Done this step

Try it for yourself

Identify a company's known contact route without using a link supplied in a suspicious message.

☐ I tried the task.

My notes

What if it really was from a company?

Checking through its official app or known contact route lets you deal with a real request without trusting the text's link.

Official help and the online guide

NCSC: reporting scam texts - <https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-text-message>

Read online: <https://plaintech-guides.pages.dev/guides/suspicious-text-pause-checklist/>