

iPhone, iPad & Android | Easy | 2 min read

iPhone and Android: spotting scam texts and fake delivery messages

Scam texts are very common in the UK. They often claim a parcel is waiting, a payment failed or your bank account is at risk. The messages look believable, so knowing the signs matters more than being technical.

Common signs of a scam text

- It creates urgency, such as "act now" or "final notice".
- It asks you to click a link or call a number you do not recognise.
- It says you owe a small redelivery or customs fee.
- It claims to be from your bank, HMRC, Royal Mail, a delivery firm or a family member with a new number.
- The sender does not know your name.
- The link looks slightly wrong, such as odd spellings or extra words.

What to do

1. **Do not tap the link.** Do not reply, even to say STOP.
2. If you are unsure, go to the company's official website or app yourself by typing its address, or call a number from a past statement or the back of your card.
3. Check whether you are expecting a delivery. Genuine firms rarely ask for card details by text.
4. Report it. In the UK, forward scam texts to **7726** (it spells SPAM). This is free.
5. Delete the message.

If you already clicked or replied

1. Do not panic. Do not enter any more details.
2. If you typed in card or bank details, call your bank straight away, using the number on your card. Ask them to stop payments.
3. If you entered a password, change it on the real site, and anywhere else you use it.
4. Run a check for suspicious apps, especially on Android.
5. Report to Action Fraud, the UK's national reporting centre.

When to get more help

Get help if you have paid or shared details, if you have installed an app after a text, or if you are worried a relative is being targeted. We can check your phone and help secure your accounts.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.