PODPLAN

Scams

How to spot them and what to do

What are scams?

Scams are designed to trick you into handing over money, personal information or access to your accounts. They can happen to anyone.

Criminals may sound helpful, professional or convincing. Taking time to check an unexpected request is sensible—not rude.

How scammers make contact

Scams can arrive through:

- Telephone calls, texts and messaging apps.
- Emails, social media and online adverts.
- Dating websites, shopping sites and online marketplaces.
- Letters or unexpected doorstep visits.

A familiar name, convincing logo or number on your caller display does not prove who is contacting you. Even voices and videos can be faked.

Warning signs

Pause if someone:

- Pressures you to act immediately.
- Asks you to keep the conversation secret.
- Says your money is at risk and must be moved.
- Offers guaranteed returns or unusually easy money.
- Requests passwords, PINs, security codes or access to your device.
- Asks for an unexpected payment or changes bank details.
- Wants payment by gift card, cryptocurrency or another unusual method.
- Becomes threatening or tries to stop you checking with someone else.

Poor spelling can be a warning sign, but many scams use polished, professional language.

Common scams

"Your bank account is at risk"

Someone pretending to be your bank or the police asks you to transfer money to a "safe account", withdraw cash or hand over your card.

Do not move money or hand anything over. End the conversation and contact your bank independently.

"Hi Mum, I've lost my phone"

A message claims to be from a relative using a new number and asks for urgent help paying a bill. A caller may even sound like someone you know.

Check using the person's usual number or another trusted route before sending money.

Unexpected bills, refunds or delivery charges

A message claims you owe tax, need to pay a delivery fee or can claim a refund or benefit. The link may lead to a fake website.

Use the organisation's official website or app instead of following the message's link.

Investment and pension offers

An advert or caller promises unusually high returns, special access or a limited-time opportunity. Criminals may impersonate genuine financial firms.

Check the firm and its permissions using the FCA Firm Checker. Contact it using the details shown there—not those supplied by the caller.

https://www.fca.org.uk/consumers/fca-firm-checker

Friendship and romance scams

Someone builds a relationship online, then asks for money for an emergency, travel or an investment.

Do not send money because someone you have only met online asks for it. Talk the request through with someone you trust.

Doorstep and repair scams

An unexpected visitor claims your roof, boiler or driveway needs urgent work, or says they must enter to check something.

Keep the door closed while you check. Contact the organisation using a number you find independently. Do not agree to work under pressure.

Fake technical support

A caller or pop-up claims your computer or account has a problem and asks you to install software or allow remote access.

Do not give an unexpected caller access to your device or online banking.

Stop, check, then decide

1

Stop the conversation

You can hang up, close the message or refuse entry. You do not need to explain or apologise.

2

Check independently

Use a number from your bank card, a genuine statement or an official website you already trust. Do not use contact details or links supplied in the suspicious message. If you received a suspicious landline call, use another phone where possible.

3

Protect your details

Do not share passwords, PINs or one-time security codes with someone who contacts you unexpectedly. Never approve a payment or security request you did not initiate.

4

Talk it through

Ask someone you trust before making an unexpected payment or a major financial decision. A genuine organisation should allow you time to check.

If you think you have been scammed

1. Contact your bank immediately

If you sent money, shared payment details or see an unfamiliar transaction, contact your bank or payment provider through a trusted route.

Explain what happened. Ask it to protect your accounts, try to stop or recover the payment, and explain any reimbursement rights. **Getting money back is not guaranteed.**

---

2. Secure affected accounts

If you shared a password, change it through the genuine website or app. Change it anywhere else you used the same password and switch on two-step verification where available.

If someone accessed your device, stop using it for banking until you have obtained trusted technical help. Contact your bank from another device.

---

3. Keep evidence

Save messages, emails, receipts, payment details and screenshots. Note dates, telephone numbers and what was said. Keep this information secure.

4. Report it

England, Wales and Northern Ireland: Report fraud or cybercrime to **Report Fraud**, which has replaced Action Fraud.

https://www.reportfraud.police.uk
0300 123 2040

Scotland: Contact **Police Scotland on 101**.

If someone is in immediate danger, call 999.

---

5. Watch for a second scam

Criminals may contact you again claiming they can recover your money for a fee. Do not pay someone who contacts you unexpectedly promising recovery.

Reporting suspicious messages

You can report suspicious contact even if you have not lost money.

- **Emails:** forward to **report@phishing.gov.uk**.
- **Texts:** forward to **7726**, free of charge.
- **Mobile calls:** text **7726** with the word **Call**, followed by the suspicious caller's number.
- **Messages in an app:** use the app's reporting and blocking tools.

Keep any evidence you may need before deleting or blocking.

Helping someone else

Listen without blame. Scammers deliberately manipulate trust, fear and urgency.

Offer to help the person contact their bank and report what happened. Agree practical steps together, respecting their choices and privacy.

© 2026 Lumen Later Life Living Pty Ltd. All rights reserved. Podplan® is a registered trademark.