

PRINT IT. KEEP IT HANDY. MAKE A FAMILY PLAN.

1 SPOT THE WARNING

Pause before acting.



Unexpected message
Verify independently.



Urgent payment
Pressure is a warning sign.



Too-good offers
Check claims and details.



Secrecy requests
Do not hide suspicious transfers.

2 VERIFY INDEPENDENTLY

Use trusted routes.



Contact directly
Use an official number you find.



Check website
Type the address yourself.



Ask a second person
A pause can prevent loss.



Avoid gift cards
Never pay surprise fees this way.

3 PROTECT ACCOUNTS

Reduce your risk.



Use strong passwords
Unique for each account.



Turn on MFA
Add a second login check.



Keep details private
Never share one-time codes.



Update devices
Install trusted security updates.

4 IF YOU PAID

Act quickly.



Call your bank
Use the official fraud number.



Keep evidence
Save messages and receipts.



Secure accounts
Change passwords from a safe device.



Report locally
Use official fraud reporting channels.

MY FAMILY PLAN:

Local alert source: _____ Emergency contact: _____

SCAMS: STOP BEFORE YOU PAY — SAFETY NOTES

Keep this page with your visual quick-glance guide.

1 IMPORTANT NOTE 1

Scammers may impersonate banks, government, relatives or delivery firms. Caller ID, logos and websites can be faked.

2 IMPORTANT NOTE 2

Never share one-time authentication codes, passwords or remote access to your device with an unexpected caller.

3 IMPORTANT NOTE 3

If money was sent, contact your bank or payment provider immediately using a verified channel. Recovery is not guaranteed; beware of recovery scams.

4 IMPORTANT NOTE 4

Reporting routes vary by country. Use official police, consumer protection or national fraud-reporting services.

MAKE IT PRACTICAL

Write your own local emergency number, contact details and relevant official alert service on page 1. Review the guide with your household.

OFFICIAL REFERENCE POINTS (check local rules):

consumer.ftc.gov/scams

ncsc.gov.uk/collection/phishing-scams

actionfraud.police.uk