

*In a world full of disinformation, get **Clarity**.*

SCAM CLARITY · LARGE, CLEAR PRINT

Spot the Scam

A guide for older relatives and the families who look out for them: phone, doorstep, romance, investment, bank and parcel scams, and exactly who to call

If in doubt: hang up, wait and check



START HERE

About this guide



Scams can fool anyone. This guide is written for older readers, in large print and plain words, and for the sons, daughters, grandchildren, neighbours and carers who want to help them stay safe.

Part one: Why scammers target older people.
Know the tricks

Part two: Phone.
The scams to know

Part three: How to start the conversation
For families without upsetting anyone.

Part four: If The first hour.
it happens

OUR PROMISE

In a world full of disinformation, get Clarity. Every phone number in this guide was checked on the organisation's own official website in October 2026. Every figure comes from an official or published source, named at the end of each chapter. Numbers can change, so if one does not work, look it up on the organisation's own website.

This guide is written for Scotland first, with the right numbers for England, Wales and Northern Ireland too. For general information only. It is not legal or financial advice.

CONTENTS

In this guide

KNOW THE TRICKS

1	Why scammers target older people	8
2	The four warning signs	14
3	The pressure tricks scammers use	19

THE SCAMS TO KNOW

4	Phone scams	25
5	Bank, police and courier scams	31
6	Doorstep scams and rogue traders	36
7	Parcel and delivery scams	41
8	Romance scams	45
9	Investment and pension scams	49
10	Texts, emails and “Hi Mum” messages	54
11	Scam mail, prizes and fake charities	59

FOR FAMILIES

12	Starting the family conversation	64
13	A family safety plan	68
14	Signs that someone is being scammed	73

IF IT HAPPENS

15	If you think you have been scammed	78
16	Getting your money back	82
17	Beware the recovery scam	87
18	Free help and support	90
●	My important numbers	94
●	Worksheets and checklists	96
●	Words explained	103
●	Useful contacts	105
●	Sources	107

The whole guide on one page



The golden rule

If anyone contacts you out of the blue and asks for money, bank details, a code or personal information: **stop**. Say no, end the call or close the door, and check with someone you trust.

● Six things to remember

- **Your bank and the police will never** ask you to move money, hand over cash or cards, or tell them your PIN.
- **Hang up and wait five minutes**, or use a different phone, before you call anyone back.
- **Call 159** to reach your bank safely. It cannot be faked.

- **Never pay at the door** and never agree to work on the doorstep.
- **Never send money to someone you have only met online**, however kind they seem.
- **Being scammed is not your fault.** Tell someone, and report it. It helps you and protects others.

● Who to call

Your bank	159, or the number on the back of your card
------------------	---

Police Scotland	101, or 999 in an emergency
------------------------	-----------------------------

Consumer advice (Scotland)	consumeradvice.scot: 0808 164 6000
-----------------------------------	------------------------------------

Age Scotland helpline	0800 12 44 222
------------------------------	----------------

PART ONE

Know the tricks

Why scammers target older people, how to spot a scam in seconds, and the pressure tricks they rely on



IT IS NOT YOUR FAULT

Why scammers target older people

Scammers are criminals who do this as a full-time job. Many work in organised gangs, with scripts, fake websites and stolen personal details. Falling for one of their tricks says nothing about how clever you are.

● Who gets scammed?

People of every age are scammed. Younger people often lose money buying things online that never arrive. Older people are more often targeted by phone, at the door and by post, and when they do lose money, they tend to lose more.

Scammers often go after older people because they believe:

- you may have savings, a pension pot or a home with no mortgage
- you are more likely to be at home and to answer the landline
- you were brought up to be polite, and will not just hang up
- you may live alone, with nobody nearby to talk it over with
- you may feel embarrassed and not tell anyone afterwards

None of these things are weaknesses. Politeness, trust and kindness are good qualities. Scammers simply take advantage of them. This guide gives you permission to be “rude” to anyone who contacts you out of the blue asking for money.

WHAT THE EVIDENCE SAYS

Fraud is now the most common crime. The Crime Survey for England and Wales estimated **4.5 million fraud incidents** in the year to March 2026, and about 7.8% of adults were victims in a single year.

Losses are at record levels. UK Finance, which collects figures from the banks, reported that criminals stole **£1.28 billion** through payment fraud in 2025. Losses to investment scams rose 40% to £221.5 million, and romance scam losses rose 23% to £39.2 million.

In Scotland, Age Scotland reports that 400,000 older people living in Scotland have been targeted by scammers.

Older people lose more when it happens. The US Federal Trade Commission, which keeps one of the

largest scam databases in the world, found that people aged 60 and over were less likely than younger adults to report losing money, but people in their 80s who did lose money lost the most.

● **Why people stay silent**

Age Scotland lists the most common reasons people do not report scams: embarrassment, fear of being judged, believing nothing can be done, and not wanting to worry the family. Every one of these helps the criminals. When scams are reported, banks can block accounts, police can track gangs and warnings can go out to others.

IF IT HAS ALREADY HAPPENED

If something has already happened to you, turn to Part four now. Acting quickly can make a real difference, and nobody will think less of you.

● A word for families

Memory problems and dementia can make a person easier for scammers to fool. Researchers in Chicago followed 935 older people for about six years and found that those with **low awareness of scams** had a higher risk of later developing Alzheimer's dementia or mild memory problems. That does not mean that being scammed is a sign of dementia. It does mean that a sudden change in how someone handles money or post is worth a gentle, caring conversation (see Part three).

Sources: ONS, Crime in England and Wales: year ending March 2026 (fraud section); UK Finance, Annual Fraud Report 2026; Age Scotland, Avoiding Scams guide (April 2026) and “Speaking up about scams”; US Federal Trade Commission, Protecting Older Consumers 2024–2025 (December 2025); Boyle PA et al., “Scam awareness related to incident Alzheimer dementia and mild cognitive impairment”, Annals of Internal Medicine, 2019 (doi.org/10.7326/M18-2711).



The four warning signs

Scams change all the time, but almost every scam has at least one of these four signs. Learn them and you can spot a scam you have never seen before.

1. Out of the blue

A call, text, email, letter or knock at the door that you were not expecting.

2. In a hurry

“Act now”, “today only”, “or you will be arrested”. Rushing you stops you thinking.

3. Keep it secret

“Don’t tell your bank.” “Don’t tell your family.” Secrecy protects the criminal, not you.

4. Money or details

They want a payment, cash, your card, your PIN, a password or a code sent to your phone.

● Take Five to Stop Fraud

Take Five is the national campaign run by the banks and UK Finance. Its advice fits on a fridge magnet:

Stop

Take a moment to stop and think before parting with your money or information. It could keep you safe.

Challenge Ask yourself: could it be fake?
It is OK to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

Protect Contact your bank straight away if you think you have been scammed, and report it to the police.

Take Five also has a useful phrase: **master the art of impoliteness.** When someone is asking for your money or personal information, being “rude” might be the safest thing you can do.

EVEN THE SCAM-BUSTERS GET COPIED

Criminals sometimes pretend to be Take Five itself. Take Five says it will never text or call you and ask you to share your information or transfer money.

WHAT THE EVIDENCE SAYS

Banks and police forces all give the same core advice because the same patterns turn up again and again in real cases. The Financial Conduct Authority (FCA) says that if you have been contacted out of the blue, are being pressured to act quickly, or are promised returns that sound unrealistic, you should be “extremely cautious”. Police Scotland’s list of things it will **never** ask you to do includes keeping contact with the police a secret.

● The “pause” habit

The single most useful habit is to **pause** before you do anything with money. A real bank, a real tradesman and a real friend will all still be there in an hour. A scammer will not.

WHAT YOU COULD SAY

“I never make decisions about money on the phone. Give me your name and I will call your company back on the number I have.” Then hang up.

Sources: Take Five to Stop Fraud, takefive-stopfraud.org.uk (checked October 2026); FCA, “Crypto investment scams” (updated 16 February 2026); Police Scotland, “Police impersonation fraud”.



The pressure tricks scammers use

Scammers are not magicians. They use a small set of tricks over and over again. Once you can name the trick, it loses its power.

● **Trick 1: Pretending to be someone you trust**

They say they are from your bank, the police, HMRC, the council, a delivery firm, your energy company, or a well-known shop. They may already know your name, address and the name of your bank, because personal details are bought and sold by criminals. The phone number on your screen can be faked

(this is called **number spoofing**), so a call can look as if it comes from your bank's real number.

● **Trick 2: Fear**

“Your account has been hacked.” “You owe tax and a warrant is out for your arrest.” “Your grandson has been in an accident.” Fear makes it hard to think clearly. That is exactly why they use it.

● **Trick 3: Hurry**

The clock is always ticking: the money will be lost tonight, the offer ends today, the engineer is only in the area this morning. Real organisations give you time.

● **Trick 4: Kindness and flattery**

Romance scammers and fake “investment advisers” can be patient, warm and attentive for weeks or months.

They remember your birthday and ask about your health. The kindness is a tool.

● **Trick 5: Isolation and secrecy**

They tell you not to speak to bank staff, or give you a story to tell the cashier, such as “say it is for a new kitchen”. Police Scotland says it will never ask you to memorise lines to say if bank staff ask you questions.

● **Trick 6: A small yes first**

A tiny payment, a “confirmation” of your date of birth, or a code read out “just to check”. Each small yes makes the next, bigger request easier.

WHAT THE EVIDENCE SAYS

UK Finance’s 2026 report says investment scams are being driven by fake adverts and social media posts

offering big returns, and that victims of investment scams usually take longer to realise they have been scammed than victims of other scams. In romance scams, victims made an average of almost **10 payments** each before the scam was stopped, which shows how scammers build up slowly. Police Scotland now also warns about **voice cloning**: criminals using digital tools to copy a person's voice so they can pretend to be them on the phone.

Name the trick

When you feel pressure, ask yourself:

- Is someone pretending to be a person or company I trust?
- Am I being made to feel frightened, rushed or flattered?
- Am I being told to keep it secret?
- Is this a small first step towards money?

Sources: UK Finance, Annual Fraud Report 2026 (investment and romance scam sections); Police Scotland, “Police impersonation fraud” and “Voice cloning scams” (scotland.police.uk/advice/scams-and-frauds/).

PART TWO

The scams to know

Phone calls, bank and police impersonation,
doorstep traders, fake parcels, romance,
investments, texts, emails and post



Phone scams

The phone is still the tool scammers use most for reaching older people. A friendly voice, a convincing story and a number on the screen that looks real.

● The calls to watch for

“Your bank account is at risk” They want you to move your money to a “safe account”. There is no such thing. See the next chapter.

“This is the police” They ask for your help with an investigation, or say your bank staff are corrupt. Then they ask for cash, cards or a transfer.

“Your computer has a problem”

A “technician” wants you to install a program so they can control your computer, then asks for payment or bank details.

“You owe tax”

They threaten arrest or court unless you pay today. HMRC says a genuine call will not threaten arrest or rush you.

“Press 1”

A recorded message tells you to press a key to speak to someone about your bank, broadband or an Amazon order.

“Grandma, it’s me”

A relative who says they are in trouble and needs money now. Their voice may even sound right.

● **Number spoofing**

Criminals can make a call look as if it comes from a real number, even your bank's. **Never trust the number on the screen.** If you are worried, hang up and call back on a number you find yourself.

● **Why you should wait before calling back**

Some scammers keep the line open after you hang up, then play a dialling tone so that when you call “your bank”, you are still talking to them. Wait at least five minutes, call a friend first to clear the line, or use a different phone such as a mobile.

● **The safe way to call your bank: 159**

159 is a short number run by Stop Scams UK. It connects customers of more than 99% of UK high street

current accounts safely and directly to their bank, and it **cannot be spoofed**. If you get an unexpected call about money, hang up and dial 159.

WHAT THE EVIDENCE SAYS

Reports of scam phone calls pretending to be from HMRC fell by 97% during 2021, from 79,477 in March to 2,491 in December, after HMRC worked with phone companies to stop most of its helpline numbers being spoofed and to shut down numbers used by scammers. That shows two things: spoofing is real, and blocking it works. HMRC's head of cyber security operations put it simply: "HMRC will never ring up threatening arrest, only criminals do that."

Police Scotland lists phone scams and voice cloning, where criminals copy someone's voice, among the main scam types it deals with.

WHAT YOU COULD SAY

“I don't deal with anything over the phone. I'll call my bank myself.”

Then put the phone down. You do not need to explain or say goodbye.

● Fewer nuisance calls

- Register your landline and mobile with the **Telephone Preference Service** (TPS): call 0345 070 0707 or go to tpsonline.org.uk. It is free and stops most legal sales calls. Scammers ignore it, so stay alert.
- Ask your phone company what free call-blocking it offers. Many can block withheld or international numbers.

- Let calls from unknown numbers go to the answerphone. A genuine caller will leave a message.
 - Never press a number on a recorded message you were not expecting.
-

Sources: Stop Scams UK, “159 phone number” (stopscamsuk.org.uk/159); GOV.UK, “Scam HMRC call reports drop by 97%” (HMRC, 21 January 2022) and “Report scam HMRC messages, calls and social media accounts”; Police Scotland scams and frauds advice; Telephone Preference Service, tpsonline.org.uk (all checked October 2026).



Bank, police and courier scams

These scams cost people their life savings. The criminal pretends to be from your bank or the police, frightens you, and then “helps” you protect your money by giving it to them.

● How a “safe account” scam works

- 1.** You get a call, often with your bank’s number on the screen. The caller says there is fraud on your account.
- 2.** They know some of your details, which makes them sound real.
- 3.** They tell you staff at your branch may be involved, so you must not tell anyone.

4. They ask you to move your money to a new “safe account” to protect it. The account belongs to the criminal.
5. Sometimes they ask for a code that has been texted to you, which lets them into your account or approve a payment.

● **Courier fraud**

In courier fraud, a “police officer” or “bank investigator” asks you to help catch a criminal. You are asked to withdraw cash, buy gold or foreign currency, or hand over your bank card and PIN to a courier who comes to your door. There is no investigation, and the courier is part of the gang.

● What the police will never ask

Police Scotland says it will **never** ask you:

- for your bank card PIN number or online banking login details
- to transfer money from your account, withdraw cash, or buy foreign currency
- to give cash or bank cards to anyone
- to pay a fine or fee to it or a third party over the phone or online
- to memorise lines to say if bank staff ask you questions
- for remote access to your phone, computer or other devices
- to keep contact with the police a secret

If someone says they are a police officer and you feel uncomfortable, stop talking. Take their name and shoulder number, then call **101** from a different phone to check.

WHAT THE EVIDENCE SAYS

UK Finance's figures show that impersonation scams, where criminals pose as a bank, the police or another organisation, fell again in 2025, with losses down 12%. Banks say warnings, the 159 number and staff training in branches are helping. But these scams remain among the most damaging, because the sums involved are often a person's whole savings.

Remember

Your bank will never ask you to move money to keep it safe. Nobody genuine will ever send a courier to collect your cash, card or PIN.

WHAT YOU COULD SAY

“I don’t move money or hand over cards for anyone. I’m going to hang up and call my bank on 159.”

Sources: Police Scotland, “Police impersonation fraud” (scotland.police.uk, checked October 2026); UK Finance, Annual Fraud Report 2026 and press release; Take Five to Stop Fraud.



Doorstep scams and rogue traders

A knock at the door: “I was passing and noticed some loose tiles on your roof.” Doorstep criminals are often confident, charming and pushy, and they may work in pairs.

● Two kinds of doorstep crime

Bogus callers

People who pretend to be from the council, a charity, the water or energy company, or even the police, to get into your home and steal money or valuables.

Rogue traders

People who offer work you do not need, such as roofing, guttering, driveways, tree cutting or garden work. They want cash quickly, and the work is never done, or done badly, or the price suddenly goes up.

Keep yourself safe

- You do not have to open the door. Use a door viewer, a window or a camera, and a door chain or bar.
- Keep your doors locked, even when you are at home.
- Only let in visitors with an appointment.
- Check ID, but remember ID can be faked. Close the door and call the company on a number you look up yourself.

- Ask them to come back later when someone else can be with you.
- **Never** agree to work on the doorstep, and **never** pay upfront in cash.
- Never go to the bank with a trader, or let one drive you there.
- Lock away cash and valuables.

IF THEY WILL NOT GO

If they will not leave, or you feel threatened, call **999**. If you can, write down what they look like and the make, colour and registration number of their vehicle.

● Your right to cancel

If you agree to buy goods or services worth more than £42 at your home, the law usually gives you **14 days to cancel**. The trader must tell you about this right

in writing. If they do not, the cancellation period can be extended. Contact [consumeradvice.scot](https://www.consumeradvice.scot) for help.

WHAT THE EVIDENCE SAYS

Police Scotland advises keeping doors locked, using a chain or viewer, checking ID by calling the company, and asking callers to come back when someone else is there. It also warns that scammers often target the same person more than once, so anyone who has already been caught out should be extra careful. Trading Standards Scotland treats doorstep scammers as one of its priority areas.

WHAT YOU COULD SAY

“No thank you. I don’t buy at the door.” Then close the door. You do not need to give a reason.

● Get help in Scotland

consumeradvice.scot 0808 164 6000,
Monday to Friday
9am to 5pm. Free
advice about traders,
run by Advice Direct
Scotland with
Trading Standards.

Police Scotland 101 to report it, or
999 if you feel
threatened or they
will not leave.

Sources: Police Scotland, “Rogue traders and doorstep crime”; GOV.UK, “Door to door sales” and The Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013; consumeradvice.scot contact page; Trading Standards Scotland, tsscot.co.uk (all checked October 2026).



Parcel and delivery scams

“We tried to deliver your parcel. Please pay a small fee to rearrange.” These messages arrive by text and email by the million, especially before Christmas.

● What they look like

- “We couldn’t deliver your package. Please pay a fee.”
- “Your parcel is waiting for collection. Click this link.”
- “Customs charges are due on your item.”
- A link that looks odd, is shortened, or does not end in the company’s real web address.

The fee is usually small, such as a pound or two, so it does not feel risky. But the real aim is to get your **card details**, which are then used to steal much more, or for a follow-up phone call from a fake “bank” saying your card has been misused.

● **What Royal Mail says**

Royal Mail says it will only text or email you about a parcel if the sender asked for tracking updates. It will not:

- ask for your bank details, passwords or personal data
- ask for payment for an underpaid item by email or text. Instead, it leaves a grey “Fee to Pay” card through your door. (It may also text or email about customs charges if the sender gave your details.)

- send email attachments unless you asked for them
- ask you to enter details on a website that is not part of Royal Mail

WHAT THE EVIDENCE SAYS

Royal Mail's own "Is this real?" checklist asks four questions. Did you ask for tracking updates? Does the message ask for money or personal information? Does the link look unusual or shortened? Do you feel pressured or rushed? Purchase scams, which include many fake delivery and shopping scams, made up 71% of all scam cases reported by the banks in 2025.

● What to do

1. Do not click the link, scan any QR code, or reply.

2. Check by going to the delivery company's website yourself, or using the tracking number from the shop you bought from.
3. Forward scam texts to **7726** (free). Royal Mail also asks for a screenshot sent to reportascam@royalmail.com.
4. If you typed in card details, call your bank on 159 straight away.

Sources: Royal Mail, "Scam advice" (royalmail.com/help/scam-protection, checked October 2026); UK Finance, Annual Fraud Report 2026 (purchase scams).



Romance scams

Romance scammers make people feel loved, then use that love to take their money. They are patient, kind and attentive, and many of the people they target are widowed, divorced or lonely.

● How it usually goes

- 1.** You meet someone online: on a dating site, on Facebook, in a game or even in a comment thread. Their photos are attractive, often stolen from someone else.
- 2.** They quickly say how strongly they feel about you and ask to move the chat to WhatsApp, text or email, away from the site.

3. They have a reason they cannot meet or video call: working on an oil rig, serving in the army abroad, a doctor with a charity, a broken camera.
4. After weeks or months, a crisis appears: a medical bill, a visa, a plane ticket, a parcel stuck in customs, or an “investment” they want to share with you.
5. The first request is small. Then there is always another.

● **Warning signs**

- ☐ They say “I love you” very quickly.
- ☐ They never manage to meet you or video call.
- ☐ Their stories do not quite add up, or their photos look too professional.
- ☐ They ask you to keep the relationship secret.

☐ They ask for money, gift cards, crypto, or for you to receive and send on money or parcels for them.

The one rule

Never send money, or share your bank details, with someone you have not met in person, however long you have been talking and however real it feels.

WHAT THE EVIDENCE SAYS

Romance scams reached a record high in 2025. UK Finance reported **£39.2 million** lost across **6,335 cases**, up 23% on the year before. On average, each victim made almost **10 payments** before the scam was stopped, which shows how slowly and patiently these criminals work. UK Finance also reported cases where a fraudster went as far as marrying the victim to keep stealing money.

● If it might be happening to someone you love

Do not mock or lecture. The feelings are real, even if the person is not. Ask gentle questions: “Have you been able to video call?” “Would you mind if we did a quick image search on their photo together?” Offer to help them check, and keep the door open. See Part three for more.

Sources: UK Finance, Annual Fraud Report 2026 (romance scams) and BBC News report on it; Police Scotland, “Romance fraud” (scotland.police.uk/advice/scams-and-frauds/romance-fraud/, checked October 2026).



TOO GOOD TO BE TRUE

Investment and pension scams

Investment scams are now the biggest cause of scam losses in the UK. They offer high returns with little risk, in shares, gold, property, wine, carbon credits or crypto. The investment does not exist.

● How they find you

- Adverts on social media and search engines, often with fake celebrity endorsements or fake news stories.
- Cold calls from smooth “brokers” with posh-sounding firm names, sometimes copying the name of a real firm.
- Letters and glossy brochures.

- A new online “friend” or romantic partner who wants to show you how they made money.

● **The signs**

- ☐ You were contacted out of the blue.
- ☐ You are promised high returns, or told there is “no risk”.
- ☐ There is pressure: “only a few places left”, “the price goes up tomorrow”.
- ☐ A website shows your money growing fast, but when you try to take it out there are fees, taxes or excuses.
- ☐ They want payment by bank transfer to a personal account, or in crypto.

● Check before you invest: the FCA's free tools

FCA

Warning List

Search for firms the FCA knows are operating without permission or running scams: fca.org.uk/consumers/warning-list-unauthorised-firms

Financial Services Register

Check a firm is authorised, what it is allowed to do, and its **real** phone number and address: register.fca.org.uk

FCA

Consumer Helpline

0800 111 6768, if you are worried about a firm or think you have been contacted by a fraudster.

● Pensions

Cold calls about pensions are banned in the UK. If someone calls you out of the blue about your pension, offering a free

review, early access before age 55 or a special investment, it is almost certainly a scam. Hang up. For free, impartial help with a pension, use **MoneyHelper**, the government-backed service, at moneyhelper.org.uk.

WHAT THE EVIDENCE SAYS

UK Finance reported **£221.5 million** lost to investment scams in 2025, a record and a rise of 40% in a single year, with almost 15,000 cases.

Investment scams made up 38% of all losses where people were tricked into sending money. UK Finance says they are being driven by fake adverts and social media posts, and that victims often take a long time to realise what has happened. The FCA says reports to it about crypto investment scams have more than doubled since 2020.

WHAT YOU COULD SAY

“I never invest with anyone who contacts me first. I’ll check you on the FCA Register and call you back on the number listed there.”

Sources: UK Finance, Annual Fraud Report 2026 (investment scams); FCA, “Crypto investment scams”, “Warning List of unauthorised firms” and “Report a scam” ([fca.org.uk](https://www.fca.org.uk), checked October 2026); GOV.UK, ban on pensions cold calling (in force since January 2019); MoneyHelper, moneyhelper.org.uk.



Texts, emails and “Hi Mum” messages

Scam texts and emails copy real logos and real wording. They want you to click a link, open an attachment, or reply with your details.

● Common scam messages

- “Unusual activity on your bank account. Click here to secure it.”
- “You are due a tax refund.” HMRC says it never uses texts or emails to tell you about a tax rebate or penalty.
- “Your TV licence, energy bill or phone bill payment has failed.”
- “You have an unpaid parking or road fine.”

- “Hi Mum, I’ve broken my phone, this is my new number. Can you help me pay a bill?”

● “Hi Mum” and “Hi Dad” messages

A message arrives from an unknown number, claiming to be your son, daughter or grandchild with a new phone. Soon they need money urgently for a bill they cannot pay from the new phone. **Always ring your relative on the number you already have for them**, or ask a question only they would know. Agree a family password (see Part three).

● What to do

1. Do not click links, open attachments or reply.

2. Forward scam texts to **7726** (free from most UK mobiles; it spells SPAM on the keypad). Then delete them.
3. Forward scam emails to **report@phishing.gov.uk**. The National Cyber Security Centre checks them and takes down scam websites.
4. Fake HMRC texts can also be forwarded to **60599**, and fake HMRC emails to **phishing@hmrc.gov.uk**.
5. If you want to check, go to the organisation's website yourself or call a number you already trust.

IF YOU ALREADY CLICKED

Clicked a link and typed in a password? Change that password straight away, on the real website, and anywhere else you use it. Gave bank or card details? Call your bank on 159.

WHAT THE EVIDENCE SAYS

The National Cyber Security Centre says it had removed more than **454,000 scam web addresses** by July 2026, many of them reported by members of the public forwarding emails. It acts on every message it receives. HMRC said it moved from being the third most-copied brand in the world for scam emails to outside the top 100, partly thanks to people reporting what they received.

● Safer passwords

The NCSC recommends making passwords from **three random words**, like a short, odd sentence only you would think of, and turning on **2-step verification** for email and banking, so a stolen password alone is not enough.

Your email password matters most, because it can be used to reset all the others.

A HELPING HAND

You can ask everyday AI tools like Grok to explain a confusing message or a word you do not understand. Never paste in passwords, codes or bank details, and never rely on any tool to tell you a message is safe. If in doubt, ask a person you trust.

Sources: NCSC, “Phishing scams: how to spot and report them” and “Top tips for staying secure online” (ncsc.gov.uk, checked October 2026); GOV.UK, “Report scam HMRC messages, calls and social media accounts” and HMRC, “Scam HMRC call reports drop by 97%”.



Scam mail, prizes and fake charities

Scam letters still land on doormats every day: prize draws, lotteries, psychics, miracle health cures and requests from “charities”. Some people end up on so-called “suckers’ lists” that criminals sell to each other, and receive dozens a week.

● Signs of scam mail

- ☐ You have “won” a prize or lottery you never entered.
- ☐ You must pay a fee, tax or delivery charge to claim it.
- ☐ It is addressed personally but feels oddly over-friendly, or says you have been “specially chosen”.

- ☐ A psychic or clairvoyant has an urgent message about your future, if you send money.
- ☐ It asks you to keep it confidential.

You cannot win a lottery you have not entered, and a genuine prize never needs a fee.

● What to do

- Do not reply or send money. Replying tells the criminals your address is “live”.
- Report scam mail to Royal Mail using its online scam mail form, or ask Citizens Advice on **0808 223 1133**.
- Families: if a relative is getting lots of this mail, see the signs in Part three. Friends Against Scams has trained

“Scam Marshals”, volunteers who collect and send in scam mail to help Trading Standards.

● Fake charities

Before giving to a charity that contacts you, check it on the Scottish Charity Regulator’s register at **oscr.org.uk** (or the Charity Commission for England and Wales). Give through the charity’s own website, not through a link sent to you.

WHAT THE EVIDENCE SAYS

Royal Mail asks people to report scam letters through its online form, and to contact Citizens Advice for help.

National Trading Standards runs Friends Against Scams and its Scam Marshals scheme, which aims to take away the blame and shame scam victims often feel and to help people spot and report scams.

Sources: Royal Mail, “Scam advice” (scam mail form, Citizens Advice 0808 223 1133); Friends Against Scams, friendsagainstscams.org.uk (a National Trading Standards initiative); Scottish Charity Regulator, oscr.org.uk (all checked October 2026).

PART THREE

For families

How to talk about scams without upsetting anyone, a simple family safety plan, and the signs that someone is being scammed



Starting the family conversation

The aim is not to frighten anyone or take away their independence. It is to make scams something the family talks about openly, like the weather, so that nobody ever feels too embarrassed to ask, “Does this look right to you?”

● Before you start

- **Pick a calm moment**, not straight after a scare or in front of others.
- **Start with a story** rather than a lecture: a news item, a scam text you got yourself, or this guide.
- **Share your own near-misses.** It shows that scams catch everyone, including you.

- **Treat it as teamwork.** “Let’s look out for each other” works better than “I’m worried about you.”

● **Conversation starters**

TO OPEN THE SUBJECT

“I got the strangest text today pretending to be from the bank. Have you had any like that?”

TO SUGGEST A PLAN

“I read that criminals are pretending to be grandchildren on the phone now. Shall we pick a family password, just in case?”

TO AGREE A CHECK-IN

“If anyone ever asks you for money or your bank details, would you ring me first? I’d do the same with you.”

● Things to avoid

Instead of saying...	Try...
“How could you fall for that?”	“These people are professionals. It happens to thousands of people.”
“You can’t be trusted with money any more.”	“Would it help if we went through the post together sometimes?”
“You should have known.”	“Thank you for telling me. Let’s sort it out together.”
“Don’t answer the phone.”	“Let unknown numbers go to the answerphone, and call back only on numbers you trust.”

WHAT THE EVIDENCE SAYS

Shame keeps victims quiet, and silence helps criminals. Age Scotland says the most common reasons people do not report scams are embarrassment, fear of judgement, thinking nothing can be done, and not wanting to worry family members.

Friends Against Scams asks people to help Friends Against Scams was set up partly to “take away the blame and shame that scam victims so often feel”. A family that talks openly makes it far more likely that a scam is caught early, before money leaves the account.

● **Respect their choices**

An adult who has capacity has the right to make their own decisions, including ones you would not make. Your role is to inform, support and be there, not to take over. If you are seriously worried that someone can no longer manage their money safely, see the chapter on the family safety plan for Power of Attorney.

Sources: Age Scotland, “Speaking up about scams”; Friends Against Scams, friendsagainstsams.org.uk (checked October 2026).



A family safety plan

Ten minutes spent together on a simple plan can stop a scam in its tracks. Fill in the worksheet at the back of this guide and keep it by the phone.

● 1. Agree a trusted person

Choose one or two people to ring whenever something feels wrong, before any money moves. Write their numbers on the “My important numbers” page.

● 2. Pick a family password

Choose a word or phrase that only your family knows, and is not on social media. If someone calls or messages claiming to be a relative in trouble, ask

for the password. A real relative will know it. A scammer, even one copying a voice, will not.

● **3. Make the phone safer**

- Register with the Telephone Preference Service (0345 070 0707).
- Ask the phone company about free call blocking.
- Put trusted numbers into the phone's contacts, so you know who is calling.
- Store **159** in the contacts as “My bank – safe line”.

● **4. Make the front door safer**

- Fit a door chain or bar and a door viewer.
- Put a “No cold callers” sticker on the door. Your council or Trading Standards may supply one, and some areas have “No Cold Calling Zones”.

- Agree that a neighbour or relative can be called to be there when any trader visits.

● **5. Ask the bank about extra protection**

Banks offer different tools, so ask yours what it has. Options can include lower daily payment limits, extra checks on large or new payments, turning off features you do not use, or letting a trusted person see statements. Friends Against Scams lists things you can ask your bank to apply to your account if you are worried.

● **6. Think about Power of Attorney**

A Power of Attorney lets a person choose someone they trust to help with money and property if they ever need it. It has to be set up while the person can

still make that decision. In Scotland, Powers of Attorney are registered with the **Office of the Public Guardian (Scotland)**: publicguardian-scotland.gov.uk, 01324 678300. Age Scotland suggests it as a sensible step for anyone who may be at particular risk of scams.

WHAT THE EVIDENCE SAYS

Police Scotland advises families to help protect vulnerable relatives by watching for large cash withdrawals, being alert to strange vans in the area, making it less obvious that someone lives alone, and being extra alert if they have been scammed before, because scammers often target the same person more than once. Age Scotland recommends Power of Attorney for anyone at particular risk.

Sources: Police Scotland, “Rogue traders and doorstep crime”; Age Scotland, Avoiding Scams guide (April 2026), including Office of the Public Guardian (Scotland) contact details; Friends Against Scams; Telephone Preference Service (all checked October 2026).



Signs that someone is being scammed

People being scammed often do not realise it, or are too embarrassed to say. Families, friends, neighbours and carers are often the first to notice that something is not right.

● Signs in the home

- ☐ Piles of post about prizes, lotteries, psychics or catalogues.
- ☐ Lots of unusual parcels arriving, or cheap goods they did not want.
- ☐ New building work that looks poor, unfinished or very expensive.
- ☐ Unfamiliar people or vans calling at the house.

☐ The phone ringing far more than usual, or calls they rush to take in private.

● **Signs with money**

☐ Large or regular cash withdrawals, or a sudden shortage of money for bills or food.

☐ Talk of a big win, a special investment or a new friend who needs help.

☐ Buying gift cards, gold or crypto for the first time.

☐ New loans or credit cards, or bank letters about unusual activity.

☐ Changes to bank details, wills or who has access to accounts.

● **Signs in the person**

☐ Secretive, anxious, withdrawn or defensive when money comes up.

- ☐ Talking a lot about someone they have met online but never in person.
- ☐ Saying “the bank told me not to tell anyone”, or repeating a story they have been given.

WHAT THE EVIDENCE SAYS

Researchers following 935 older people in Chicago found that low awareness of scams was linked with a higher later risk of Alzheimer’s dementia and mild memory problems, even after taking account of their thinking skills at the start. The scientists stressed that a scam questionnaire cannot diagnose anyone. But it suggests that a change in how someone deals with scams and money can be an early sign that they may need more support, and is worth a gentle word with their GP.

● What to do if you are worried

1. Talk to them kindly and privately.
Start with concern, not blame.
2. Look at the post, bank statements or messages together, if they agree.
3. If money has gone, follow the steps in Part four straight away.
4. Call the Age Scotland helpline (0800 12 44 222) or [consumeradvice.scot](https://www.consumeradvice.scot) (0808 164 6000) for advice.
5. If you think someone is being targeted or exploited and cannot protect themselves, you can contact the local council's social work team, or Police Scotland on 101. In an emergency, call 999.

Sources: Police Scotland, "Rogue traders and doorstep crime"; Age Scotland, Avoiding Scams guide; Boyle PA et al., Annals of Internal Medicine 2019 (doi.org/10.7326/M18-2711) and US National Institute on Aging summary.

PART FOUR

If it happens

What to do in the first hour, how to get money back, how to avoid being scammed twice, and who can help



ACT QUICKLY

If you think you have been scammed

First: it is not your fault, and you are not alone. Second: act quickly.

The sooner the bank knows, the better the chance of stopping payments and getting money back.

● The first hour

- 1. Stop.** Do not send any more money or details, whatever you are told. End all contact with the scammer.
- 2. Call your bank.** Dial **159**, or the number on the back of your card. Use a different phone if you can, or wait five minutes. Tell them exactly what happened.

- 3. Change passwords** for any account you think the scammer may know, starting with your email.
- 4. Report it to the police.** In Scotland, call Police Scotland on **101**, report online at scotland.police.uk, or call **999** if the crime is happening now or you are in danger. In England, Wales and Northern Ireland, report to Report Fraud at reportfraud.police.uk or on **0300 123 2040**.
- 5. Tell someone you trust.** A friend or relative can help with the calls and the paperwork.
- 6. Keep everything:** letters, texts, emails, web addresses, phone numbers and receipts. Write down what happened while you remember it.

IF THEY TOOK CONTROL OF YOUR COMPUTER

If you let a scammer connect to your computer or phone, switch off the internet (or unplug the router) and ask a trusted person or a reputable local repair shop to check the device before you use online banking again.

● Write it down

Date and time	
How they contacted me	
Who they said they were	
Phone number, email or website	
What I paid or told them	
Bank told, and reference number	

Police told, and crime reference number	
--	--

WHAT THE EVIDENCE SAYS

The banks' own figures show that speed matters. In 2025, banks returned 48% of the money lost to investment scams and 78% of the money lost to purchase scams to victims, helped by new reimbursement rules (see the next chapter). Police Scotland and the National Cyber Security Centre both advise keeping web addresses, messages and emails, because they help investigators.

Sources: Take Five to Stop Fraud; Police Scotland, "Contact us" and scams and frauds advice; Report Fraud, reportfraud.police.uk; NCSC, "Report a scam email"; mygov.scot, "Reporting online crime to the police"; UK Finance, Annual Fraud Report 2026 (all checked October 2026).



Getting your money back

If you were tricked into sending money by bank transfer, you now have strong rights to get it back. Since October 2024, banks must refund most victims of this kind of scam.

● **Bank transfer scams (“authorised push payment” scams)**

If you were tricked into making a payment yourself by Faster Payment or CHAPS, from a UK account to another UK account, the Payment Systems Regulator’s rules mean:

Who is covered Individuals, very small businesses and charities, for payments made on or after 7 October 2024.

How fast You can usually expect a refund within 5 working days. If the bank needs more information, it must decide within 35 working days.

How much Up to **£85,000** per claim. Banks can choose to pay more.

The excess Banks may take off an excess of up to £100. They cannot do this for vulnerable customers.

Time limit Claim within **13 months** of the last payment to the scammer.

If you are refused

You can complain to the bank, then take it to the Financial Ombudsman Service, which is free.

● **Card payments and stolen cards**

If someone used your card or account without your permission, or you paid by card for something that never came, tell your bank straight away. Card payments have their own protections, and your bank will explain what applies.

● **Cash, gift cards and crypto**

Money handed over in cash, gift cards or crypto is much harder to recover. Report it anyway: to the police, to your bank, and for gift cards, to the company that issued the card as quickly as possible.

WHAT THE EVIDENCE SAYS

The Payment Systems Regulator set the £85,000 limit expecting that it would fully cover 99.8% of claims by number. If a victim is vulnerable, and that affected their ability to protect themselves from the scam, the bank cannot refuse on the grounds that they were careless, and cannot take an excess. UK Finance reported that in 2025, banks returned £106.5 million of the £221.5 million lost to investment scams.

TELL THE BANK EVERYTHING

Tell the bank about anything that made you more vulnerable at the time, such as a bereavement, illness, memory problems or loneliness. It can affect how your claim is handled, and you will not be judged for it.

Sources: Payment Systems Regulator, “APP fraud reimbursement protections” and PS25/5 consolidated policy statement (psr.org.uk, checked October 2026); UK Finance, Annual Fraud Report 2026.



Beware the recovery scam

People who have lost money are often targeted again, by someone promising to get it back. Their details are sold on between criminals.

● **How recovery scams look**

- A call or email from a “lawyer”, “fraud recovery agency” or “government department” that says your money has been found.
- A “police officer” who needs a fee to release the money.
- An offer to buy back your worthless shares or investment, if you pay a charge first.
- Social media adverts for “hackers” who can trace stolen money.

The rule

Never pay anyone to get your money back. The police, your bank and the Financial Ombudsman Service never charge victims a fee.

WHAT THE EVIDENCE SAYS

The FCA warns that once someone has invested in a scam, fraudsters may target them again or sell their details to other criminals, and that the follow-up scam may include an offer to get the money back, or to buy back the investment after paying a fee. Police Scotland also warns that scammers often target the same person more than once.

WHAT YOU COULD SAY

“I’m dealing with this through my bank and the police. Don’t contact me again.” Then hang up and tell your bank about the call.

Sources: FCA, “Crypto investment scams” (If you have been scammed); Police Scotland, “Rogue traders and doorstep crime” (checked October 2026).



Free help and support

Being scammed can leave people feeling shocked, ashamed, angry or low. These organisations are free, kind, and used to helping people in exactly this situation.

● Friends Against Scams

Friends Against Scams is a National Trading Standards initiative that aims to protect people from scams and to take away the blame and shame victims often feel. Anyone can do its free short online awareness session, and it also has a free app with scam alerts and tools. Families, community groups and

carers can become “Friends” or “SCAMchampions”. Find it at **friendsagainstscams.org.uk**.

● **Advice and support in Scotland**

Victim Support Scotland

0800 160 1985. Free emotional and practical support for anyone affected by crime. Monday to Friday 8am to 8pm, weekends 10am to 4pm.

Age Scotland helpline

0800 12 44 222, Monday to Friday 9am to 1pm. Free, confidential advice for older people, carers and families, plus a friendship line.

consumeradvice.scot 0808 164 6000,
Monday to Friday
9am to 5pm. Free
consumer advice,
working with Trading
Standards.

Police Scotland 101, or 999 in an
emergency.

● For anyone in the UK

Your bank 159

**Take Five
to Stop
Fraud** takefive-stopfraud.org.uk:
advice from the banks.

**FCA
Consumer
Helpline** 0800 111 6768, about
investment firms and scams.

**Report
Fraud** England, Wales and Northern
Ireland: 0300 123 2040 or
reportfraud.police.uk.

WHAT THE EVIDENCE SAYS

Victims of fraud can feel the effects long after the money has gone. Age Scotland reminds people that the most important things are to act quickly and to report the crime, and that there is no need to feel embarrassed. Talking to someone, whether a relative, a friend or a support line, is part of recovering.

Sources: Friends Against Scams

(friendsagainstscams.org.uk); Victim Support Scotland (victimsupport.scot/contact); Age Scotland (agescotland.org.uk/contact-us); consumeradvice.scot/contact; Police Scotland; FCA; Report Fraud. All numbers and opening hours checked on each organisation's own website in October 2026.

FILL IN AND KEEP BY THE PHONE

My important numbers



Who	Phone number
My bank (back of my card)	
Bank safe line	159
Police Scotland (non-emergency)	101
Emergency	999
consumeradvice.scot	0808 164 6000
Age Scotland helpline	0800 12 44 222
Victim Support Scotland	0800 160 1985
My trusted person	
Another trusted person	

Our family password is kept	(somewhere safe, not written here)
------------------------------------	------------------------------------

If anyone calls, texts or knocks and asks for money or details, I will ring my trusted person first.

Worksheets and checklists



● Before I pay anyone: six questions

- ☐ Did I contact them first, or did they contact me?
- ☐ Am I being rushed, frightened or flattered?
- ☐ Have I been told to keep it secret?
- ☐ Have I checked the company on a number I found myself?
- ☐ Have I talked it over with someone I trust?
- ☐ Would I be happy to tell my bank exactly why I am paying?

● Red flags: if I tick any of these, I stop

- ☐ Someone I do not know contacted me first.
- ☐ I am asked to move money to a “safe account”.
- ☐ I am asked for my PIN, password or a code from a text.
- ☐ Someone wants to collect cash or my bank card.
- ☐ I am asked to pay by bank transfer, gift cards or crypto.
- ☐ I have won something I never entered.
- ☐ Someone I have only met online needs money.
- ☐ A trader at the door wants paying today.

☐ Someone offers to get back money I lost, for a fee.

KEEP A NOTE

Call and visit log



Write down any unexpected call, message or visit about money. It helps you spot patterns, and helps the bank or police if you need them.

Date	Who said they were calling	What they wanted

--	--	--

FOR FAMILIES

Our family plan



Our trusted people	
We have picked a family password (yes / no)	
TPS registered (yes / no)	
Call blocking set up (yes / no)	
159 saved in the phone (yes / no)	
Door chain and viewer fitted (yes / no)	
Asked the bank about extra protection (yes / no)	

Power of Attorney discussed (yes / no)	
We will next talk about scams on	

● Notes from our conversation

PLAIN WORDS

Words explained



159

A short phone number that connects you safely to your bank. It cannot be faked.

APP scam

“Authorised push payment”: when you are tricked into sending money yourself.

Bogus caller

Someone who pretends to be from a company or the council to get into your home.

Courier fraud

A fake police officer or bank sends someone to collect your cash, card or PIN.

Phishing

Fake emails or texts that try to get your details.

Recovery scam

A second scam promising to get back money you lost, for a fee.

Rogue trader

A trader who charges too much for poor or unnecessary work.

Romance scam

A fake online relationship used to get money.

Safe account

A fake “safe” account that belongs to a criminal.

Spoofing

Faking the number that appears on your phone screen.

Two-step verification

A second check, such as a code, as well as your password.

Voice cloning

Copying someone’s voice with digital tools to pretend to be them.

ALL IN ONE PLACE

Useful contacts



Your bank	159, or the number on your card
Police Scotland	101; 999 in an emergency; scotland.police.uk
Report Fraud (England, Wales and NI)	0300 123 2040; reportfraud.police.uk
consumeradvice.scot (Advice Direct Scotland)	0800 164 6000, Mon to Fri 9am to 5pm
Age Scotland helpline	0800 12 44 222, Mon to Fri 9am to 1pm
Victim Support Scotland	0800 160 1985
Take Five to Stop Fraud	takefive-stopfraud.org.uk
Friends Against Scams	friendsagainstscams.org.uk

FCA Consumer Helpline	0800 111 6768; register.fca.org.uk
Scam texts	Forward to 7726 (free)
Scam emails	Forward to report@phishing.gov.uk
Fake HMRC messages	Texts to 60599; emails to phishing@hmrc.gov.uk
Telephone Preference Service	0345 070 0707; tpsonline.org.uk
Citizens Advice (scam mail)	0808 223 1133
Office of the Public Guardian (Scotland)	01324 678300
MoneyHelper (pensions)	moneyhelper.org.uk

FURTHER READING

Sources



Each chapter lists its own sources. All were checked in October 2026.

Official and regulator sources

Police Scotland, scams and frauds advice, including “Police impersonation fraud”, “Rogue traders and doorstep crime”, “Romance fraud” and “Contact us” (scotland.police.uk). Payment Systems Regulator, “APP fraud reimbursement protections” and PS25/5. Financial Conduct Authority, “Crypto investment scams”, Warning List and Financial Services Register. National Cyber Security Centre, “Phishing scams: how to spot and report them” and “Top tips for staying secure online”. HMRC, “Scam HMRC call reports drop by 97%” (21 January 2022) and GOV.UK scam reporting pages. GOV.UK, “Door to door sales”; The Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013. mygov.scot, “Reporting online crime to the police”. Office for National Statistics, Crime in England and Wales: year ending March 2026.

Charities and industry

UK Finance, Annual Fraud Report 2026. Take Five to Stop Fraud. Stop Scams UK, “159”. Age Scotland, Avoiding Scams (April 2026), Staying Safe Online and “Speaking up about scams”. Friends Against Scams (National Trading Standards). Victim Support Scotland. consumeradvice.scot. Trading Standards Scotland. Royal Mail, “Scam advice”. Telephone Preference Service.

Research

Boyle PA, Yu L, Schneider JA, Wilson RS, Bennett DA. Scam awareness related to incident Alzheimer dementia and mild cognitive impairment: a prospective cohort study. *Annals of Internal Medicine* 2019;170(10):702–709. doi.org/10.7326/M18-2711. US Federal Trade Commission, Protecting Older Consumers 2024–2025 (December 2025).

Illustrations

The cover, icons and ornaments were drawn by Clarity Guides. No photographs of people are used.

© 2026 Clarity Guides. For personal use. For general information only; not legal or financial advice. If you are in danger, call 999.

CLARITY GUIDES

Hang up. Wait. Check.

Phone, doorstep, romance, investment, bank and parcel scams explained in large, clear print, with a family conversation guide, worksheets and every helpline checked on its official website.

Published by Clarity Guides

*In a world full of disinformation, get **Clarity**.*

