
STOP | CHECK | CALL
2026 EDITION
DON'T CLICK, DON'T PAY, DON'T PANIC!
Fraudsters count on you rushing. You win by taking your time!
A Practical Scam-Safety Guide for Adults Aged 60 and Over
Spot scams before they start
Protect your money and identity
Avoid costly mistakes
Stay confident online and on the phone
Get help fast if something goes wrong
Because peace of mind is priceless.
RECOGNISE THE RED FLAGS
CHECK BEFORE YOU ACT
VERIFY INDEPENDENTLY
PROTECT YOURSELF
TALK TO SOMEONE
Real scam examples
Expert tips
Easy checklists
Step-by-step guidance
YOU DON'T HAVE TO BE A TECH EXPERT TO OUTSMART A SCAMMER.
We make it simple!
WRITTEN FOR 60+ AND THEIR LOVED ONES
PRACTICAL. SIMPLE. TRUSTED.
Rasool M.A.
Author of Practical Guides that Empower You to Stay Safe and Confident
Peace of mind is priceless.

DON'T CLICK, DON'T PAY, DON'T PANIC

A Simple Guide to Spotting Scams, Protecting Your Money, and Staying Confident Online and on the Phone

For anyone who wants to feel a little more sure of themselves

Contents

Before Anything Else

If someone is asking you right now for money, a code, or access to your computer, here is what to do:

1. Don't click. Don't pay. Don't panic.

Whatever you're being asked to do — stop. You do not have to decide right now.

2. Hang up, or step away from the message.

A real bank, company, or family member will always let you check and call them back. Nobody genuine will mind you taking a moment.

3. Check it yourself.

Find the phone number or website yourself — from a bank card, a bill, or by typing the address in yourself. Never use a number or link someone has just sent you.

4. Talk to someone you trust.

Call your bank, the police, or a family member or friend. Asking for a second opinion is never embarrassing — it's simply sensible.

> **REMEMBER**
>
> *Don't click. Don't pay. Don't panic. In that order, every time.*

A Word Before We Start

This booklet is not about how easily someone could fool you. It's the opposite. It's a set of simple habits that make you very hard to fool, once you know them.

Scammers don't target people because they're careless, confused, or bad with technology. They target people because they've had years of practice creating pressure — pretending to be a bank, a grandchild, the police, or a new friend. It can happen to anyone, at any age, and it is never the victim's fault.

Every chapter in this book ends the same way: don't click, don't pay, don't panic. That's really the whole method. Everything else is just examples, so you can recognise it when it happens to you.

REMEMBER

Scammers are skilled at creating pressure. Being deceived is not a sign of anything wrong with you.

How Scammers Try to Rush You

Almost every scam relies on one or more of these feelings. Once you can name them, they lose most of their power.

Urgency

“You must act in the next ten minutes.” Genuine organisations almost never demand an instant decision about money.

Fear

“Your account has been hacked” or “You're under investigation.” Fear makes it harder to think clearly — that's exactly why it's used.

Secrecy

“Don't tell your bank” or “Keep this between us.” A genuine organisation never asks you to hide a conversation from the people meant to protect you.

Kindness and flattery

Warmth and attention, especially from someone new online, can be manufactured just as easily as fear.

Repeated contact

Being called again and again is designed to wear down your resistance. It is a warning sign, not proof that something is genuine.

🚩 **RED FLAG**

If a conversation feels rushed, frightening, secretive, or suspiciously flattering — that feeling is the warning.

CHAPTER 1

“This Is Your Bank”

One of the most common and convincing scams is a phone call from someone claiming to work for your bank's fraud or security team. You're told your account has been compromised, and that the only way to protect your money is to move it to a new “safe account.”

This is always false. No genuine bank will ever ask you to move your money to another account to protect it. Your money is already safe exactly where it is.

> **SCAM EXAMPLE:** *"This is your bank's security team. We need you to move your savings to a protected account immediately."*

WHAT TO SAY: *"I will hang up and call my bank myself, using the number on my card."*

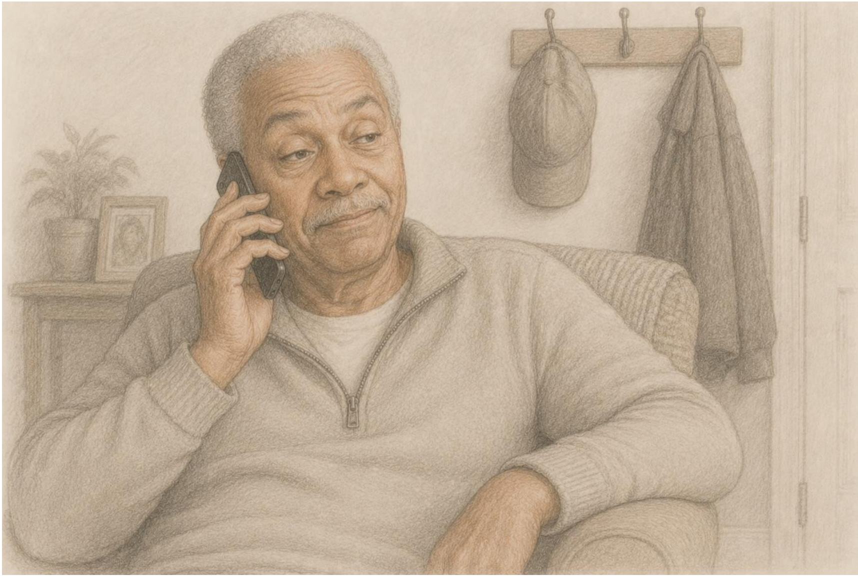
Scammers may also ask you to read out a one-time code that's just arrived by text, or to approve something in your banking app. Never do this. A code exists to prove that YOU are making a transaction — never to prove that someone else is genuine. No bank employee will ever need you to read one aloud.

🚩 **RED FLAG**

A bank will never ask you to move money to a "safe account," or ask you to read out a security code.

CHAPTER 2

“This Is the Police”



Scammers sometimes pretend to be police officers, tax officials, or other government workers. They may say you're wanted for questioning, that your identity has been used in a crime, or that you owe an urgent payment.

Genuine police and government agencies will never ask you to withdraw cash, hand money to a courier, buy gift cards, or keep the matter secret from your family.

> **SCAM EXAMPLE:** *"This is Detective Reyes. We need your help catching a corrupt bank worker — please withdraw your savings in cash."*

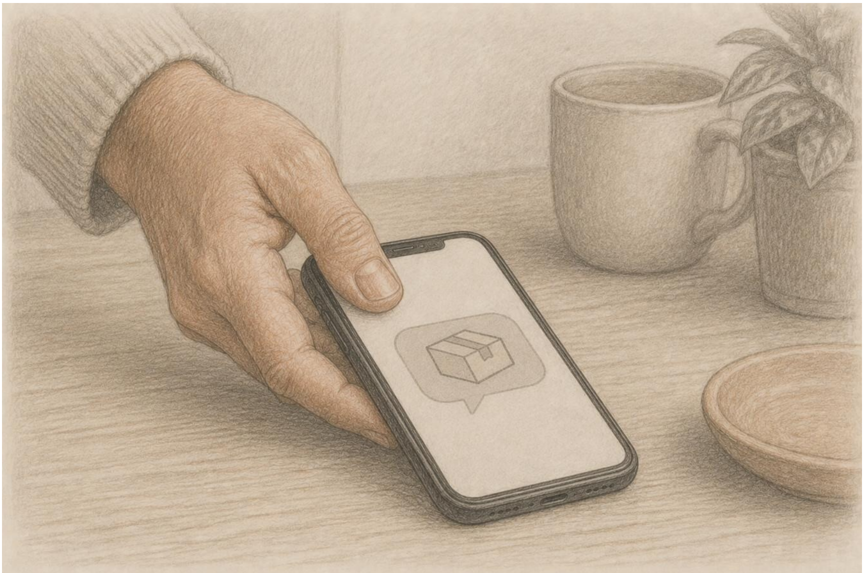
> **WHAT TO SAY:** *"I'll call the police myself, using their official non-emergency number."*

A genuine letter or call from a tax office, court, or benefits agency will always tell you how to check it independently — through their official website or phone number, never a link or number they've given you.

> **A LITTLE HUMOUR**
>
> *The police will not ask you to buy gift cards. They already have plenty of stationery.*

CHAPTER 3

The Parcel, the Refund, and the Text You Weren't Expecting



Short text messages and emails about undelivered parcels, unpaid tolls, or tax refunds are some of the most common scams, precisely because they're quick and easy to click on without thinking.

> **SCAM EXAMPLE:** *"Your parcel could not be delivered. Pay £1.99 to rebook delivery: [link]"*

A genuine delivery company will never threaten to destroy or return your parcel within a few hours. If you're expecting a delivery, go to the courier's official website yourself, rather than clicking the link in the message.

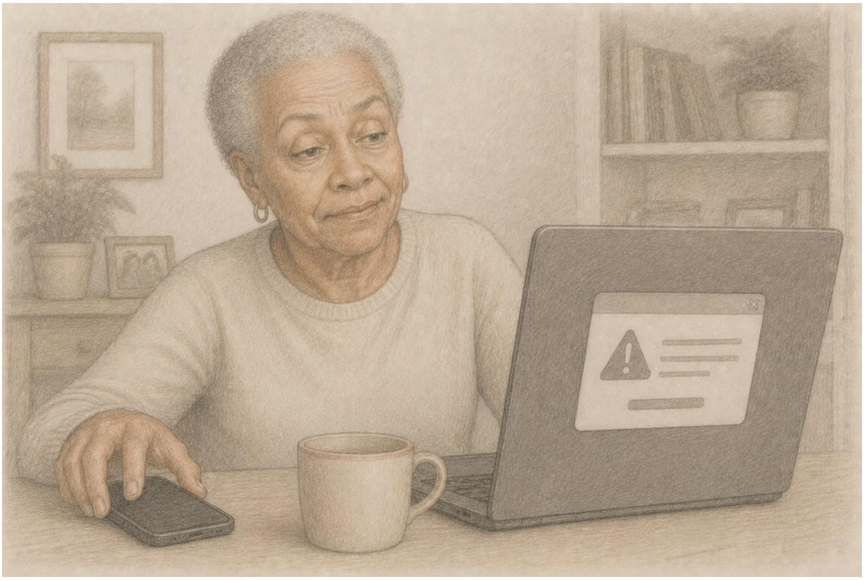
The same goes for QR codes — the square black-and-white patterns you scan with your phone's camera. A QR code can lead absolutely anywhere, and there's no way to tell where until it's too late. If in doubt, type the website address in yourself instead of scanning.

SAFE NEXT STEP

Type the address yourself, instead of clicking a link or scanning a code.

CHAPTER 4

“Your Computer Has a Virus”



This scam usually starts with an alarming pop-up message on your screen, or an unexpected phone call, saying your computer is infected and that help is available right now — often by allowing someone to take remote control of your device.

Genuine technology companies do not contact you first about a virus. If you see a frightening pop-up, don't call any number it shows you. Simply close the window, or turn your computer off and on again.

🚩 **RED FLAG**

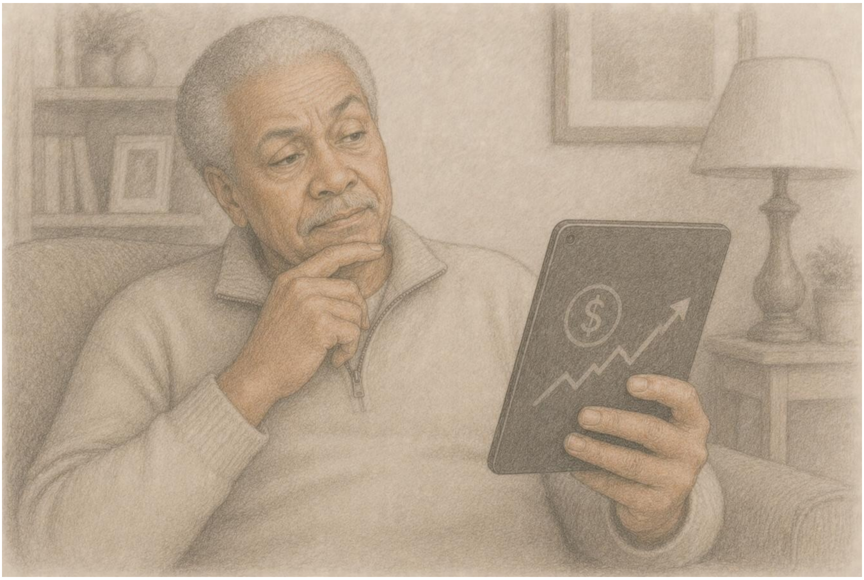
A real company will never contact you first to warn you about a virus.

If you've already let someone access your device:

- Turn off your Wi-Fi or unplug your router.
- Don't log into any accounts on that device for now.
- From a different device, call your bank to let them know.
- Change your passwords from that other device.
- Ask someone you trust, or a reputable local technician, to check the computer.

CHAPTER 5

Guaranteed Riches Before Lunch



Investment scams often begin with an advertisement on social media, promising extraordinary and “guaranteed” returns. You may be shown a fake trading app with numbers that keep rising — all invented.

> **SCAM EXAMPLE:** *"Turn £500 into £5,000 in 48 hours — guaranteed returns, as seen on TV."*

A common trick is to let you make one small, genuine withdrawal early on, to build your confidence, before asking for larger deposits. When you try to withdraw the bigger amount, you'll suddenly be told a “fee” or “tax” must be paid first. That fee will never actually release anything.

There is no such thing as a guaranteed investment. Anyone promising one — including a stranger, a celebrity endorsement, or a slick-looking app — is not telling the truth.

A LITTLE HUMOUR

If a stranger promises guaranteed riches before lunchtime, lunch is probably the only guaranteed part.

If you've already lost money this way, be careful of a second approach afterwards: someone offering, for a fee, to help you "recover" what you lost. This is almost always another scam, aimed specifically at people already known to have been targeted once.

🚩 **RED FLAG**

Anyone who contacts you offering to recover lost money, for an upfront fee, is very likely running a second scam.

CHAPTER 6

Meeting Someone Special Online

Meeting new people online — through dating websites, matchmaking apps, or social media — is completely normal, at any age, and many real relationships begin this way.

Unfortunately, some people create entirely fake profiles, using photographs that aren't really theirs, hoping to meet someone open to companionship. This is called romance fraud, and it is never a sign that someone was foolish or too trusting. It's a sign that a criminal invested real time and effort into a convincing performance.

How the story usually unfolds

- A fast, flattering connection — compliments and shared interests appear quickly.
- A suggestion to move the conversation off the dating site, onto texting, email, or a phone call.
- Weeks or months of daily messages and talk of a shared future, building trust.
- Eventually, a believable problem appears — often involving money.

🚩 **RED FLAG**

A relationship that's moved fast, moved off the original website, and now involves money or secrecy deserves a pause.

When Love Asks for Money

The request for money rarely comes on the first day. It usually arrives once real trust has been built, wrapped in a reasonable-sounding story — a medical emergency, a stuck business deal, unexpected customs or legal fees, or a request to receive and forward money "temporarily."

> **WHAT TO SAY:** *"I don't send money to anyone I haven't met in person. Let's talk once we've met, or once I've spoken to my bank and a family member."*

The "almost here" trip

One version of this scam is especially common: plans are made to finally meet in person, and then, close to the date, something goes wrong. A flight is delayed and needs a rebooking fee. A visa or "proof of funds" payment is suddenly required. Customs has "held" a piece of luggage and wants a release fee. Each new problem asks for one more, usually modest, payment — reasonable-feeling each time, but adding up quickly.

> **SCAM EXAMPLE:** *"Customs has stopped my case at the airport. I just need £300 to release it before my connecting flight."*

A real journey never needs a series of private payments sent to a personal bank account, a gift card, or a cryptocurrency wallet. A genuine visitor's biggest travel problem is usually overhead luggage space — not a customs officer who conveniently only accepts gift cards.

TAKE YOUR TIME

Before paying anything travel-related, look up the airline or customs authority's own website yourself — never use a link or number the other person has sent you.

You're Allowed to Ask Questions

If anything in this chapter feels familiar, there's no need for embarrassment. These stories are often built carefully over months by people who do this for a living.

Before sending money to anyone met only online:

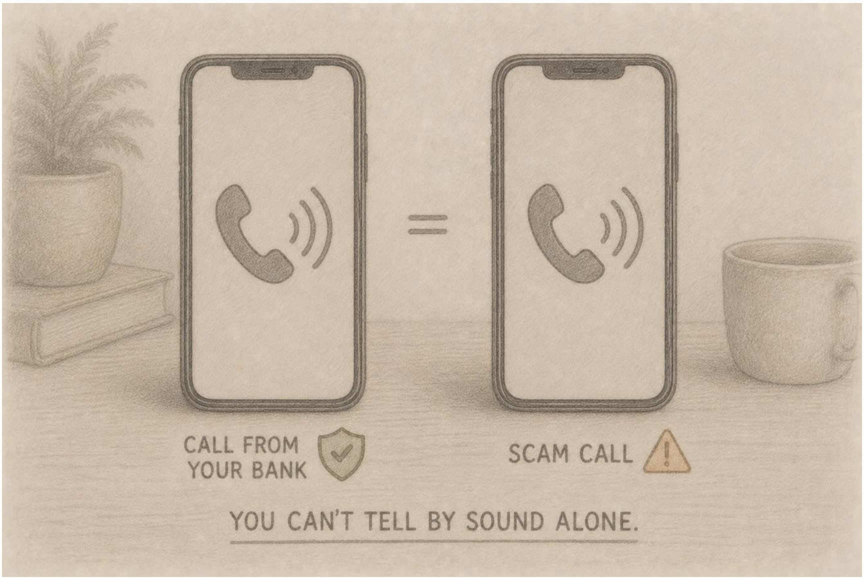
- Don't click or pay yet.
- Search for their photograph online — it may appear under a different name.
- Ask whether a video call is possible.
- Tell a trusted family member or friend about the relationship and the request.

Telling someone you trust about an online relationship is not a betrayal of it. If it's genuine, it will still be there after the conversation. And a partner who's never once been free for a video call, after months of daily messages, may simply have terrible Wi-Fi — or may not be who the photograph suggests.

> **ASK SOMEONE**
>
> *There is no shame in asking a trusted person what they think. It's one of the most sensible safety steps there is.*

CHAPTER 7

The Voice That Sounds Just Like Them



New technology can now copy someone's voice convincingly from just a short recording — sometimes taken from a video posted online. Combined with a phone number that's been faked to show a family member's name, this can feel completely real in the moment.

If you get a distressing call — a supposed accident, arrest, or medical emergency involving a family member — don't send money straight away, however urgent it sounds.

- Call that family member back on their usual number.
- Check with another relative.

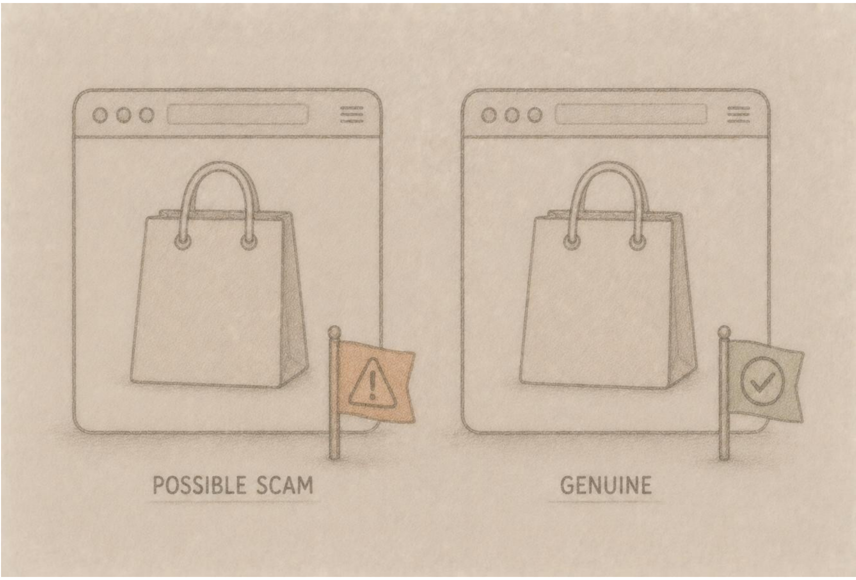
- Consider agreeing, as a family, on a private way to double-check each other in a genuine emergency.

🚩 **RED FLAG**

A voice can sound familiar and still not be real. Checking is always stronger than recognising.

CHAPTER 8

Shops, Refunds, and “Keep the Change”



Fake online shops and misleading adverts are increasingly convincing, sometimes even copying a genuine, trusted shop's design almost exactly. If a seller asks you to pay by bank transfer outside the website itself, rather than through its normal payment system, you lose your usual protections.

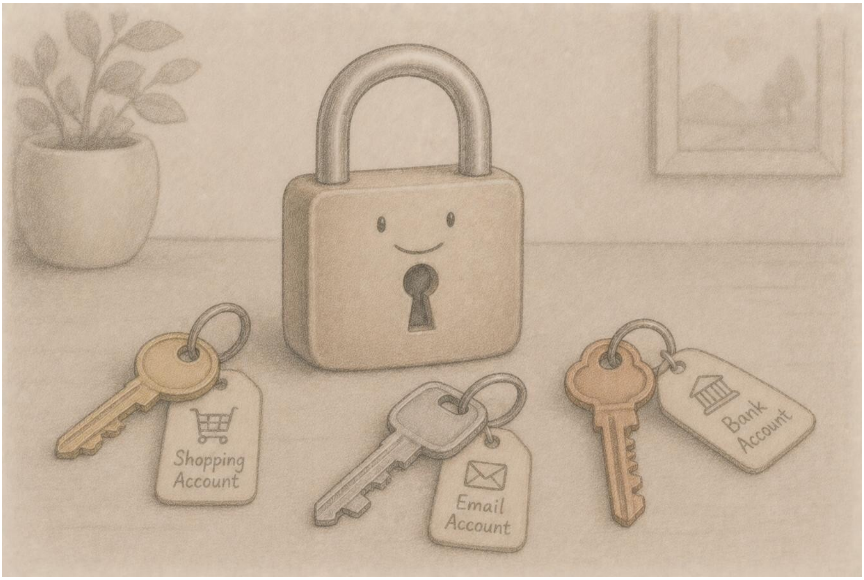
Another common trick: someone “accidentally” sends you more money than agreed and asks you to send back the difference. Days later, their original payment turns out to be fake, leaving you having sent real money for nothing.

SAFE NEXT STEP

Always wait for a payment to fully clear in your account before acting on it in any way.

CHAPTER 9

A Few Simple Habits That Help a Lot



You don't need to become a technology expert to be safe. A few small habits make a very big difference.

- Use a different password for each important account — a password manager can remember these for you, so you don't have to.
- Turn on “two-step verification” wherever it's offered. It just means a second check, usually a code sent to your phone, on top of your password.
- Keep your phone and computer updated — those updates often fix safety problems.

- Lock your phone with a code, fingerprint, or face recognition.
- Only download apps from your phone's official app store.
- Ask your bank about setting up alerts for new transactions.
- Check your bank statements regularly for anything unfamiliar.
- Keep a trusted person's phone number somewhere easy to find.

A LITTLE HUMOUR

"Password123" has already had a long and unsuccessful career. It's time to let it retire.

CHAPTER 10

If Money Has Already Gone

If you think you've sent money to a scammer, try not to feel embarrassed — just act quickly. Speed genuinely helps.

- Contact your bank or payment provider immediately, and ask for the fraud team.
- Ask whether the payment can be stopped or reversed.
- Change any passwords that may be affected, from a different device.
- Keep hold of messages, phone numbers, receipts, and screenshots.
- Report what happened to the police or your country's fraud-reporting service.

- Tell someone you trust.
- Watch out for a second scam offering to "recover" your money for a fee.
- Be kind to yourself — and ask for support if you need it.

REMEMBER

Acting quickly is the single most useful thing you can do. It was not your fault.

A Final Word: It Was Not Your Fault

If you have been scammed, or nearly were, please know this clearly: the responsibility belongs entirely to the person who deceived you, never to you.

Many people feel too embarrassed to tell their family or the police, worried about being seen as foolish or forgetful. That fear of judgement is exactly what allows scammers to keep succeeding — because embarrassed silence means nobody else is warned, and nobody is caught.

Talking about it — to a family member, a friend, your bank, or the police — is not an admission of weakness. It's one of the strongest, most sensible things you can do.

REMEMBER

Don't click. Don't pay. Don't panic. And if it's already happened — don't stay quiet.

If It Happens More Than Once

Being contacted again — or even targeted a second or third time — is not a sign that something is wrong with you, and it doesn't mean the first scam was your fault twice over.

Once your name, phone number, or email has responded to one scam attempt, it can be bought and sold between criminal groups, sometimes called a “lead list.” Being contacted again is a sign your details are circulating — not a sign that you're an easy target.

ASK SOMEONE

Tell your trusted contact about every suspicious approach, not just the ones that work. It helps them help you.

Who Else Can Help

You don't have to handle this alone, and you don't only have to rely on one family member. A few other places worth knowing about:

- Your bank may have a dedicated fraud team or “vulnerable customer” support line — ask when you call.
- Local community centres, libraries, and religious or social groups often run free scam-awareness sessions.
- Charities that support older people often run confidential helplines specifically for scam advice and emotional

support, separate from the police — for example, Age UK's free Advice Line (0800 678 1602) in the UK, or AARP's Fraud Watch Network Helpline (1-877-908-3360) in the United States.

These services exist because being deceived is common, not shameful. Trained volunteers on these lines speak to people in exactly this situation every single day.

Test Yourself: Spot the Warning Signs

Read each short scenario and see if you can spot what's wrong before turning the page. There's no pressure — this is just a chance to practise.

1. The Bank Call

You get a call from someone saying they're from your bank's security team. They already know your name and the bank you use. They say your account has been compromised and you must transfer your savings to a new “safe account” right now.

2. The Prize Text

You get a text saying you've won a supermarket gift card. To claim it, you just need to click a link and enter your card details to “confirm your identity.”

3. The New Online Friend

Someone you matched with on a dating site three weeks ago says they're falling for you. They've never managed a video call, but they've just messaged to say they're stuck at customs abroad and need £200 to release their luggage before finally flying to meet you.

4. The Grandchild in Trouble

You get a call from someone who sounds like your grandchild, saying they've been in an accident abroad and need money wired urgently — and asking you not to tell their parents.

TAKE YOUR TIME

Think about what you'd do for each one, then turn the page to check your answers.

Quiz Answers

1. The Bank Call

Warning signs: knowing your name and bank doesn't prove who they are; a real bank never asks you to move money to a “safe account.” Hang up and call your bank using the number on your card.

2. The Prize Text

Warning signs: a genuine prize never requires your card details to “confirm your identity”; unexpected prizes you didn't enter for are a classic scam. Don't click the link.

3. The New Online Friend

Warning signs: no video call after weeks of daily contact; a trip that needs a payment to happen. Don't send money — ask to see them on a video call, and tell a trusted person about the relationship.

4. The Grandchild in Trouble

Warning signs: urgency, a request for secrecy, and money requested before you've verified anything. Hang up and call your grandchild directly on their usual number, or check with another family member.

REMEMBER

If you spotted most of these, you already have the *instincts you need. The rest of this book is just practice.*

Quick Checklist — Before You Pay or Share Anything

- Did this contact reach me unexpectedly?
- Am I being asked to hurry, or to keep this a secret?
- Have I checked this using a number or website I found myself — not one somebody just gave me?
- Have I spoken to someone I trust about it?
- Would I be comfortable telling my bank exactly what I'm about to do?

If you answered “no” to checking independently — stop here. Don't click. Don't pay. Don't panic. Take your time.

Reporting Contacts — Real Examples

Every country has its own fraud-reporting service. These change occasionally, so it's worth checking the organisation's own website for the latest details — but here are some real starting points:

United Kingdom

Report Fraud (formerly Action Fraud): 0300 123 2040, or reportfraud.police.uk. For emotional support and advice: Age UK Advice Line, 0800 678 1602 (free, every day, 8am–7pm).

United States

Federal Trade Commission: reportfraud.ftc.gov, or 1-877-382-4357. For support and guidance after a scam: AARP Fraud Watch Network Helpline, 1-877-908-3360 (free, open to everyone, not just AARP members).

Canada

Canadian Anti-Fraud Centre: 1-888-495-8501, or antifraudcentre-centreantifraude.ca.

Australia

Scamwatch: scamwatch.gov.au (online reporting). For identity-theft support: IDCARE, 1800 595 160.

If you're in immediate danger, or a crime is happening right now, always call your local emergency number first.

SAFE NEXT STEP

Find your own country's official fraud-reporting website and write its number on the next page, today.

My Important Numbers

Fill this in on a quiet day, so it's ready if you ever need it.

My bank's official phone number (from my card):

____

My trusted person's name and number:

____

A second trusted person's name and number:

____

My local police (non-emergency) number:

____

My country's fraud-reporting service:

____

REMEMBER

Don't Click. Don't Pay. Don't Panic. Keep this book somewhere handy, and don't be afraid to look back at it.