# Avoiding scams Ways to protect yourself



## Information written with you in mind.

Our guides are produced with the help of older people, carers and expert peer reviewers.

Published: August 2025



# Join our Readers' Panel and have your say.

The Readers' Panel is a group of volunteers who provide vital feedback on our guides and other resources.

Their feedback helps us ensure that our information is as useful as possible for older people and their carers, family and friends.

www.ageuk.org.uk/readers-panel

This information guide has been prepared by Age UK and contains general advice only, it should not be relied on as a basis for any decision or action and cannot be used as a substitute for professional advice.

Neither Age UK nor any of its subsidiary companies or charities accepts any liability arising from its use and it is the reader's sole responsibility to ensure any information is up to date and accurate.

Please note that the inclusion of named agencies, websites, companies, products, services or publications in this information guide does not constitute a recommendation or endorsement by Age UK or any of its subsidiary companies or charities.

### **Contents**

What this guide is about	4
Types of scam	6
Doorstep scams	8
Mail scams	12
Phone scams	14
Email and online scams	18
Relationship scams	21
Identity theft	23
Investment and pension scams	26
<b>Dealing with scams</b> What if someone I know is being scammed? Reporting a scam	28 30 31
The lasting impact of a scam	33
Useful organisations	34

### What this guide is about

Being scammed can be very distressing, but it can happen to anyone. If you've been scammed, you're not alone – and there's support available.

This guide explains what you can do to protect yourself from scams and how to spot the warning signs that someone might be trying to scam you. It explains:

- the ways scammers might try to approach you
- what you can do if you think you've been scammed
- how to lower your risk of being scammed in the future.

A scam is a way of cheating someone out of their money – it's a crime. The people behind scams are sometimes referred to as fraudsters, swindlers or con artists. But in this guide, we refer to them as scammers or criminals.



All of the information in this guide applies in England. This symbol indicates where it differs for Wales and Northern Ireland. If you're in Scotland, contact Age Scotland for advice.

A scammer might approach you on your doorstep, by post, over the phone or online. New digital ways of communicating have led to an increasing number and variety of scams.

Any scam, even if you spot it in time, can leave you feeling shaken up. But this guide can help you protect yourself by knowing what to look out for, and what to do if you suspect a scam.

"I was scammed last year and it really affected my confidence. But I spoke to a friend and found out he'd had a similar experience." Alan, 66





### Good to know

It's normal to sometimes feel worried about scams. But if your worries are getting on top of you, there's lots of support available to make sure they don't interfere with your day-to-day life.

See pages 34-38 for a list of organisations that can provide trusted information and advice.

### Types of scam

This guide covers some of the most common types of scam, how to spot them and what to do next.



### **Doorstep scams**

Scammers knocking on your door pretending to be people they're not in order to get money from you.

Find out more on page 8.



### Mail scams

Post containing false claims or offers that try to steal your money.

Find out more on page 12.



### **Phone scams**

Scammers ringing up to try to get your personal information or persuade you to buy products you don't need.

Find out more on page 14.



### **Email and online scams**

Emails or fake websites pretending to be legitimate or trying to tempt you with fraudulent offers.

Find out more on page 18.



### **Relationship scams**

Scammers trying to earn your trust through a pretend relationship to get money from you.

Find out more on page 21.



### **Identity theft**

Scammers trying to get hold of your personal details to access your savings or run up debts in your name.

Find out more on page 23.



### **Investment and pension scams**

Scammers trying to steal your pension, perhaps by offering seemingly attractive but fraudulent investment opportunities.

Find out more on page 26.

### **Doorstep scams**

A scammer may knock on your door and pretend to be a trader, charity collector or someone in need of help. They may seem polite and friendly – but that doesn't mean you can trust them.

### What to watch out for

- Traders who say they've noticed something wrong with your property that they can fix.
- People who come to your door claiming to be police officers or bank staff and ask to see your PIN or your bank cards – real police officers and bank staff would never come to your house and ask for this.
- Pushy sellers who say they have large discounts, time-limited offers, or only a few items left.
- People who claim to be from gas and electricity companies but don't have an official ID badge.
- Deliveries of any goods or products that you didn't order.
- Charity collectors who seem pushy or can't supply a registered charity number.
- People who ask to come into your home because they say they need help for example, to use your phone or toilet.



### **Good to know**

If you get unwanted sales and marketing flyers through the door, you can join the Mailing Preference Service (page 37) to help reduce it.

### What to do

You don't have to open the door to anyone you don't know. If you do, always think: **Stop, Lock, Chain, Check**.

- **Stop**: Are you expecting anyone?
- Lock: If not, lock any other outer doors before answering the front door, as some scammers may work together.
- Chain: Put the door chain on and look through the window or peephole to see who's there. Remember to take the chain off again afterwards if people with a key (like a carer or cleaner) need to be able to get in.
- Check: Ask for an identity card and examine it carefully. If you're still
  not sure, phone the company the person says they're from. Get the
  number from a bill or your phone book. Don't worry about leaving
  someone waiting if they're who they say they are, they won't mind.
  If you're being pressured or you feel unsafe, contact friends, family or
  the police.



#### Who to contact

- Dial **999** in an emergency, or **101** if you want to report the incident and you're not in immediate danger.
- If you've been scammed on your doorstep, ring Citizens Advice (page 35) and let them know. They'll pass your report on to Trading Standards.
- If you suspect you've been scammed, contact Action Fraud (page 34).
- To check if someone is genuinely from your phone, energy or water supplier, call up using the number on your latest bill.
- To check if a charity is officially registered, contact the Charity Commission (page 35).



In Northern Ireland, contact the Charity Commission Northern Ireland (page 35).

"After I lost £400 to a doorstep scam, my local Age UK came and placed 'No cold callers' stickers on my door and window." Jan, 80





### Good to know

For more information about how to check someone's credentials, see pages 28-29. If you need to report a scam, see pages 31-32.

### More tips to avoid doorstep scams

There are some additional steps you can take to protect yourself from doorstep scams.

- Never buy from doorstep sellers.
- Ask for a 'No cold callers' sign from your local council or get a printable version online and put it on the front door or in the window.
- Set up a password with your utility providers to be used by anyone they send round so you can be sure they're genuine.
- Don't be embarrassed to say 'No' or to ask people to leave.
- Never sign anything on the spot take the time to think about any offer, even if it seems genuine. When it comes to things like home improvements, it's always best to get several written quotes before deciding.
- Don't accept deliveries of anything you didn't order that's addressed to you. If you accept them without realising, contact the company they were sent from or the local police.
- Never hand over your bank cards, cash, jewellery or any other valuable items to anyone claiming to be from the police or your bank.
- Remember: if it sounds too good to be true, it probably is.



### **Next steps**

See our guide **Staying safe** for more information about rogue traders and staying safe at home.

### Mail scams

Some scams are sent by post and may be addressed to you directly by name. They contain fake claims or offers that are designed to con you out of your money. It's not always easy to control what people send you – but you can control your response.

### What to watch out for

- Lotteries or prize draws claiming you've won a fortune. These often look legitimate, with barcodes or ID numbers. The letter will ask you to pay an administration fee, buy a product or call a premium-rate phone number to claim your winnings.
- Bills from companies you don't use. If you receive a bill from a
  provider and you're not sure you have an account with them, find the
  company's contact details in the phone book or online and ask them
  for confirmation. Don't use any contact information that's listed on
  the bill, as it'll likely be set up by the scammer.
- Psychics and clairvoyants who claim to have seen something in your future.
- Investment schemes that ask you to pay a fee and recruit friends or family to get a return on your investment.
- People asking for money because of unfortunate circumstances, like illness or poverty.
- Letters from a solicitor about an unclaimed inheritance often from a relative overseas that you've never heard of.

### What to do

- **Reject:** If you receive a letter you think is a scam, ignore it and throw it away. Never reply.
- **Report:** Join the Scam Marshal scheme. You send them your scam mail so they can catch criminals. You can find out more on the Friends Against Scams website (page 36).
- **Ignore:** Don't call any premium-rate phone lines. These numbers start with **09** and calls can cost up to £4 per minute.
- Verify: If you're unsure, check the details of the organisation (see pages 28-29).
- Opt out: Try to avoid being added to mailing lists. For example, when
  you register to vote, tick the box to opt out of the 'edited register'
  (also known as the 'open register'), as this can be used to send
  unsolicited marketing mail.
- **Reduce:** Register with the Mailing Preference Service (page 37). This will stop many direct-mailing companies from contacting you but not all of them.

### Who to contact

- Tell Royal Mail if you think you've received scam mail and send it to them with a covering letter (page 37).
- Report details of overseas scams to the Citizens Advice Consumer Service (page 35).
- Contact the Solicitors Regulation Authority (page 38) if you get a letter from a solicitor and aren't sure it's genuine. They can tell you if the solicitor's firm is registered and check a list of reported scams on their website.



In Northern Ireland, contact the Law Society of Northern Ireland (page 36).

### Phone scams

Scammers sometimes try to trick people over the phone – so be wary of uninvited or unexpected calls, and remember you can always hang up the phone if someone's making you feel uncomfortable.

### What to watch out for

- Calls supposedly from your bank or the police about fraudulent use of your bank cards or bank account. Scammers might ask for your PIN and tell you to give your bank card to a courier. Neither your bank nor the police would ever do this.
- Calls from someone claiming to be from the police or a 'fraud squad' asking you to help them with an investigation – for example, into a member of staff at your bank. The police would never ask you to help in an investigation like this.
- Pushy sales calls or investment opportunities that seem too good to be true.
- Calls about your computer or mobile phone. The person calling may say your device has a virus and ask you to download software to fix it. This is actually spyware – an unwanted program that runs on your computer and can give scammers access to all your online information.
- Be wary of any cold calls or texts from strange numbers offering products or services, such as pension or debt management.
- Calls claiming to be about correcting your Council Tax band or giving you a Council Tax rebate. Your council would never call you about a rebate out of the blue.

- Calls asking you to pay to renew your membership of the Telephone Preference Service (TPS) (page 38). The service is free and calls asking you to pay for it are scams.
- Calls that seem to be genuine because the caller has information about you. Just because someone knows your basic details doesn't mean they're legitimate. These details can include your name, address, your mother's maiden name and even your Direct Debits.
- Texts asking you to follow a link to fix a problem with one of your accounts or to track a parcel. These links will often take you to fake websites and get you to log in, which scammers can then use to access your information.
- Texts from someone claiming to be a family member who needs money urgently – they might tell you their phone's broken so they've switched to a new number.

#### What to do

- Say no: Ignore a caller who asks you for personal information such as your PIN or tells you that your computer has a virus. A genuine organisation will never ask you for these details over the phone, via email or in writing.
- **Report any scams**: Forward unwanted texts for free to **7726** so your mobile phone provider can flag potential scams.
- Check the line: Scammers can keep your phone line open even after you've hung up. Use a different phone, call someone you know first to check the line is free, or wait at least 10 to 15 minutes between calls to make sure that any scammers have hung up.
- **Use an answerphone**: You can use an answerphone on your landline or voicemail on your mobile to screen your calls.

### Types of scam

- Check your calls: Get a caller ID device to see who's calling. But be aware that some scammers may appear to be legitimate – for example, your bank or utility company.
- Try call blocking: Some phones have call-blocking features to stop unwanted calls. If yours doesn't, you can use a separate call blocker. Some blockers come pre-programmed with known nuisance numbers and some allow you to add numbers to that list when you get a nuisance or scam call. You can buy call blockers from various retailers and some local authorities provide them.
- Cut the cold calls: Join the free Telephone Preference Service (TPS) (page 38). This should cut the number of cold calls you receive, though it won't necessarily block all scammers. TPS has a service to stop cold calls to mobile phones too. Go to their website or text 'TPS' and your email address to 85095 to register.
- Call the company: If you get a phone call from an organisation asking you for personal information, contact the company directly using a known email or phone number to check the call is legitimate.
- Avoid links: If you've received a text asking you to follow a link, don't click on it. If you'd like to check if the text is genuine, contact the company directly either using their official website or phone number and enquire about your account that way.



### **Good to know**

A 'cold call' is a phone call out of the blue from a company or person you've never dealt with before, usually trying to sell you something. They aren't always scams, but they can be irritating.

### Who to contact

- Contact Action Fraud to report a scam (page 34).
- Contact your bank if you receive a call about your bank account or credit card that concerns you. You can call the centralised number 159 or the phone number on the back of your bank card.
- Call, text or go online to register for the Telephone Preference Service (page 38). There's a free call blocker to stop scam and nuisance calls available to those identified as most vulnerable by a doctor, Trading Standards officials or local councils.
- Report a scam WhatsApp user by opening the chat with the user you want to report, tapping on their name and then tapping 'report contact'.





### **Next steps**

Ask your landline provider about what call-blocking services they provide – these are normally free to customers.

### **Email and online scams**

Things like email and online shopping can make life a lot easier – but digital scams are becoming increasingly common and sophisticated, so it's good to know how to keep yourself safe.

### What to watch out for

- Fake websites. These often look like a trusted organisation's real
  website. For example, you could get an email claiming to be from
  your bank, which directs you to a fake website and asks you to enter
  your account details. A genuine organisation will never contact you
  out of the blue to ask you for your PIN or full password.
- Any emails from abroad asking for money. It may appear to be a stranded friend or relative asking for help but is really a scammer who has broken into ('hacked') that email address. Or it could ask you to transfer some money abroad in return for a larger reward later.
- Emails attachments you're not expecting. Some attachments contain viruses that infect your computer. These could seem to be from someone you know, but their account may have been hacked.
- Fake tax refund emails that claim to be from HM Revenue and Customs (HMRC), offering you a tax refund if you enter your details.
   The real HMRC would never email to give you a tax refund. This is a common scam and many people have had money stolen.
- Fake invoice emails that appear to be from companies you deal with regularly, or even a solicitor.
- Images, videos or audio recordings that might be fake. It's now
  possible to make digital content to look like real people and it can
  be used to trick and blackmail them or their friends and family.
- Any requests for one-time passwords (OTPs) when you aren't actively
  using a transaction or log-in process that requires it. It's probably a
  scam if anyone asks you for one via phone, email or text.

#### What to do

- Use a strong password: Always create a strong password for any online accounts. Your email account is a gateway to lots of other accounts, so always use a password you don't use for anything else.
- **Ignore attachments**: Don't open any attachments to an email unless you know they're safe.
- Leave the links: Don't click on any links within emails that claim to direct you to your bank, utility company or HMRC. Instead, always search for the website yourself.
- Check the web address: Secure websites should always start with https:// – the 's' stands for 'secure'. You should also look out for a padlock symbol next to the web address – but don't trust a padlock on the webpage itself.
- Report and delete: Report scam emails to the government's Suspicious Email Reporting Service at report@phishing.gov.uk and then make sure you delete the scam email.
- **Don't reply**: Never reply to scam emails, even to say 'No'. This will let the scammer know that your email address is active and they'll probably send you more emails.
- **Double-check**: If you get an unexpected request for payment from someone claiming to be a trusted organisation, look up their official phone number and give them a call to check.
- **Filter junk**: Check your email account is set up to filter junk (or spam) mail. This may help remove some suspicious emails from your inbox automatically.
- **Stay virus-free**: Make sure you have anti-virus software installed on your computer to protect it from viruses. Also take the time to install the built-in security measures that most internet browsers offer.

### Types of scam

- Check your preferences: When shopping online, you may be asked if you want to receive emails from the company. Make sure you tick or untick the correct box. You can also unsubscribe from any mailing list you've joined.
- **Trust your instincts:** If an online offer looks too good to be true then it probably is. Be suspicious of unusually low prices.
- **Do your research:** Only use retailers you trust for example, those recommended to you. If you're buying an item made by a major brand, you can often find a list of authorised sellers on its official website.
- **Use secure payment methods:** Always use the secure payment methods recommended by trusted online retailers.

### Who to contact

- If criminals have gained access to your accounts through an email scam, report it to Action Fraud (see page 34).
- Visit www.getsafeonline.org for more advice on how to deal with scam emails, or look at the help pages of your email account provider.



### **Good to know**

To make a strong password, try using three random words with a combination of capital letters and numbers. Don't use any words or numbers that include personal information, such as your name, street name, house number or date of birth.

The National Cyber Security Centre (page 37) provides information on how to stay safe online. Get Safe Online (page 36) also offers an online toolkit.



### Relationship scams

Social media and dating websites and apps can be great places to meet someone – but it's important to be careful. Some scammers use these platforms to win people's trust and take their money.

#### What to watch out for

- Someone asking for personal information, like your full name, address, date of birth or bank details.
- · Conversations that get personal very quickly.
- Someone who only tells you vague details about themselves, and nothing that can be fact-checked.
- Someone who quickly suggests talking by email, text or phone rather than via the platform where you met them.
- Emotional stories in which someone asks for money for example, claiming that they've fallen on hard times or that their relative is ill.
- Someone asking you to keep the relationship secret or trying to isolate you from your friends or family.
- Someone asking for money in order to come and visit you because they live far away.

### What to do

- Report and block: If you become suspicious, most dating platforms
  and social media sites will let you report a member. You should also
  be able to block any members who make you feel uneasy or unsafe.
- **Keep safe:** If you arrange to meet someone, meet them in a public place and always let someone know where you'll be.
- **Keep details private:** Don't share too much personal information, such as your full name, date of birth or bank details.
- Money matters: Don't send money to someone you've never met in person, no matter what reason they give or how long you've been speaking to them.
- Check them out: Have a good look at the person's profile and check they're genuine by putting their name, profile pictures or any phrases they repeat into your search engine with the term 'dating scam'.

#### Who to contact

If you've lost money in a relationship scam or you think you've been targeted, report it to Action Fraud (page 34).

"I found out Mum had sent over £1,000 to someone she'd met on Facebook." Amy, 64



### **Identity theft**

Identity theft is when your personal information (like your name, date of birth or address) is stolen and used to commit acts of fraud. These could be things like buying goods or taking out loans or credit cards in your name.

#### What to watch out for

- Any unfamiliar activity in your bank accounts or missing money that you can't remember spending.
- Post arriving at your house for someone you don't know.
- Changes to your credit rating for example, if you're refused a loan because your credit rating has worsened unexpectedly.
- You're told you're already claiming government benefits when you apply for them.
- You find out that a mobile phone contract has been set up in your name without your knowledge.



### **Good to know**

You can set up 2-factor authentication (2FA) to help secure your accounts. This adds an extra layer of security as it usually requires access to a device you own – for example, a unique code might be sent to your phone that you need to log in to your account.

### What to do

- Act quickly: Cancel any lost or stolen bank cards straight away. If your passport, driving licence or other personal information has been lost or stolen, contact the organisation that issued it immediately.
- Double-check: If you're waiting for a new card, PIN or identity document such as a passport and it's not delivered, alert the organisation providing it straight away.
- Watch your account: Contact your bank immediately if there are any transactions on your account you don't recognise.
- **Keep PINs and passwords safe:** Don't write them down or tell them to anyone.
- Use strong passwords: Try not to use the same password for more than one account and avoid using obvious passwords or any personal information.
- Watch your cards: Always shield your PIN and never let your cards or card details out of your sight when using them to buy something or withdraw money.
- **Stay safe online:** Make sure your computer has up-to-date security software.
- **Phone security:** Lock your mobile phone with a PIN or password. This will stop anyone getting the information on it.
- **Bin carefully:** Shred documents like bank statements and receipts before you throw them away.
- When you move: Give your new address to relevant organisations and ask Royal Mail (page 37) to redirect your post.

#### Who to contact

- Visit the identity theft section of the Action Fraud website (page 34) or call them for further information on how to prevent identity theft.
- Contact the Citizens Advice Consumer Service (page 35) for further advice.
- If your details have been stolen before, you might want to register
  with fraud prevention organisation Cifas (page 35). For a small fee, it
  will alert its members to carry out further checks if someone applies
  for credit in your name.
- Sometimes fraud can be committed using the identity of people who have died. Contact the Bereavement Register (page 34) to remove the deceased person's details from mailing lists, and the Government's Tell Us Once service (page 36) to inform all government departments of a person's death with just one call.

"I received a parcel for someone I'd never heard of. The whole thing seemed a bit dodgy so I spoke to the local police who said I'd had my identity stolen!" Jeff, 65



### **Investment and pension scams**

There are many ways that scammers persuade people to part with their pension – from promising investment opportunities to giving false information. They may call several times and could even have details of previous investments you've made.

### What to watch out for

- Any cold calls about your pension.
- Companies that offer a 'loan', 'savings advance' or 'cashback' from your pension or talk about new investment techniques.
- Offers of investments in stocks and shares in wine, jewellery, carbon credits or land, with rates of return that seem too good to be true, or pressure you to act quickly.
- Offers of 'pension reviews' or new ways to get hold of your pension income before the age of 55 in exchange for a fee – for example, by transferring your savings to a different scheme.
- Legitimate products that seem overvalued for example, shares that exist but have little or no resale value.
- Investment scheme where you pay a fee to join and then need to recruit friends or relatives to get a return.
- Offers about investments in cryptocurrency or foreign exchange trading. The Financial Conduct Authority (FCA) (page 36) doesn't regulate most cryptocurrencies, so they're not protected by the UK's Financial Services Compensation Scheme.

### What to do

- **Stay calm:** If you get calls offering you investments or access to your pension, don't feel rushed or pressured to respond.
- Don't commit: Always seek advice before making decisions.
- Stop the call: If you feel pressured or if the caller won't take no for an answer, end the conversation. Don't be embarrassed to put the phone down.
- Think about foreign fraud: Be wary of dealing with companies based overseas. They could be located there to avoid important regulatory requirements.
- Check adverts carefully: Don't buy from newspaper adverts or marketing leaflets unless you're sure they're genuine. Celebrity endorsements can't always be trusted, as they can be easily faked.
- **Listen to your doubts:** If you think the offer sounds too good to be true, it probably is.

### Who to contact

- Check whether companies are authorised by the FCA (page 36) using their tool at www.fca.org.uk/consumers/fca-firm-checker
- Check the scams warning list at www.fca.org.uk/scamsmart
- Get independent pension advice. Contact the Pension Wise service through MoneyHelper (page 37).
- You could also get advice from an independent financial adviser.
   You can find a list of registered advisers through MoneyHelper or the Personal Finance Society (page 37).
- You can report online scam ads on the Advertising Standards Authority's website (page 34).

### **Dealing with scams**

A tradesperson, company, catalogue or website may look professional and sound sincere – but how can you be sure they're legitimate? Here are some ways to check their credentials, and make sure you're not being scammed.

#### Check their contact details

- Ask for a landline number and phone it to see who answers.
- Be wary if the person only has a mobile phone number and a PO Box address – these are easy to close and hard to trace.
- Visit www.gov.uk/get-information-about-a-company to find out a company's details, including its registered address.

If the address is overseas, the usual consumer rights may not apply or could be tough to enforce.





### Good to know

If in doubt, always get further advice from the Citizens Advice Consumer Service (page 35).

### Check if tradespeople are registered and regulated

- There are various official registration schemes for tradespeople, such as the National House Building Council for builders and Gas Safe for gas engineers.
- Financial services or companies should be regulated by the Financial Conduct Authority (FCA) (page 36).
- If someone claims to be registered, check with the relevant trade organisation or the FCA if it's a financial company.

### Check reviews and recommendations

It's always best to get a reliable recommendation if you're buying a product or service. Search online for the company's name to see if there are any reviews. If it's a local business, ask trusted people you know in the area.

It's easy to make convincing business cards and websites, so they don't necessarily prove a person or company's legitimacy.

### Still not sure?

- Contact the Citizens Advice Consumer Service (page 35).
- Contact TrustMark (page 38) to find local tradespeople who comply with government-endorsed standards, or ask your local Age UK for an approved list of traders in the area. In Wales, speak to your local Age Cymru.



### **Next steps**

For more information, download **The Little Book of Big Scams** from the Metropolitan Police website (page 37) or email **cyberprotect@met.police.uk** for a copy.



### What if someone I know is being scammed?

Any tips you've read here also apply to friends and family. If you're worried that someone you know is being scammed, you should:

- look out for warning signs. The person may be getting unusually large amounts of post or spending a lot of money – or they may seem secretive or defensive about either of these things. It might help to give them some relevant advice from this guide and encourage them to report the scam.
- find support. The charity Think Jessica (page 38) can help you support someone who doesn't believe they're being scammed. There are more useful organisations listed at the back of this guide too (pages 34-38).



### **Good to know**

Our guide **Staying safe** has more information about staying safe at home, online and out and about. It might be helpful to share with any friends or relatives you're worried about.

### Reporting a scam

If you've been scammed, it's important to report it right away. If someone stole your money in the street you'd report it to the police – and it shouldn't be any different if a criminal gets access to your private accounts and steals your money.

- If it's an emergency: Always call 999 if you or someone else is in danger. You can call 101 to speak to the police if it isn't an emergency situation.
- If you've had money stolen: Contact your bank straight away by calling either the centralised number 159 or the phone number on the back of your bank card. They can cancel any cards and freeze your accounts.
- If you want to report a scam: Report it to Action Fraud (page 34) to get a crime reference number.

Action Fraud is the UK's national reporting centre for fraud and cybercrime. If you've experienced fraud of any kind, you can report it to Action Fraud over the phone or through their online reporting service. Once you've reported the crime, Action Fraud will pass the case onto the National Fraud Intelligence Bureau to investigate and give you a crime reference number.



### **Good to know**

If you think you've spotted a scam or you'd like some information on different scams, you can call the Citizens Advice Consumer Service for advice (page 35).

### Dealing with scams

The best thing you can do to protect others from scams and fraud is talk about it. Scams are constantly changing and becoming more sophisticated. By letting relevant organisations know you've been scammed, and by telling them how it happened, you can help them keep up to date with the latest scams and help protect others.

By reporting it, you might even be able to get some money back. Although this can't be guaranteed, it may be possible in certain circumstances:

- If you paid for something by credit card in a transaction that turns out to be fraudulent, your card provider may offer protection.
- If you have household insurance, your policy may also provide cover in some circumstances.
- If the scammer is traced, it may be possible to prosecute them and recover your money.



### **Good to know**

After reporting a scam, such as a suspicious text message, you may not hear anything back and you won't find out if the scammer's been caught. But reporting scams is worthwhile and really does make a difference. More people reporting scams makes it easier to stop the criminals and prevent others from being scammed in the future. Your experience can help keep other people safe from fraud.

### The lasting impact of a scam

We often talk about scams in financial terms and rarely talk about the emotional impact they can have. But they can damage our confidence and leave us feeling embarrassed, unsettled and unsure about who we can trust – so it's understandable to feel reluctant to talk about what's happened.

But if you've been scammed, it's so important to report it (see page 31) and to talk to your friends and family. It isn't anything to feel embarrassed about – scams are increasingly sophisticated and they're purposefully designed to steal your money. Scammers are experts and they're always looking for new ways to trick people – you shouldn't feel guilty.

You might worry that others will judge you or question your decision-making, especially as you get older. But the truth is anyone can be scammed. When you talk about it, you might be surprised by how many people you know have been scammed themselves.

The best way we can protect ourselves and others from scams is to report them and speak about them. The more we know, the less effective they are, and the less power scammers have.



### **Useful organisations**

### **Age UK**

We provide information and advice for people in later life through our Age UK Advice Line, publications and website.

Age UK Advice: 0800 169 65 65

Lines are open 7 days a week from 8am to 7pm.

www.ageuk.org.uk

In Wales, contact Age Cymru Advice: 0300 303 44 98

www.agecymru.wales

In Northern Ireland, contact Age NI: 0808 808 7575

www.ageni.org

In Scotland, contact Age Scotland: 0800 124 4222

www.agescotland.org.uk

### **Action Fraud**

Use the online fraud reporting service or call the helpline for advice on preventing fraud or on what to do if you've been scammed.

Tel: 0300 123 2040

www.actionfraud.police.uk

### **Advertising Standards Authority (ASA)**

Use their website to report an online scam advert. www.asa.org.uk/make-a-complaint/report-an-online-scam-ad.html

### **Bereavement Register**

Register the name and address of a deceased person to help stop unsolicited mail.

Tel: 020 7089 6403

www.thebereavementregister.org.uk

### **Charity Commission for England and Wales**

Regulates registered charities in England and Wales. Search on their website for registered charities.

Tel: 0300 066 9197

www.gov.uk/charity-commission

In Northern Ireland, contact the Charity Commission for Northern Ireland

Tel: 028 3832 0220

www.charitycommissionni.org.uk

### **Cifas**

Provides a registration service to protect people whose details have been stolen or are considered vulnerable.

www.cifas.org.uk

### **Citizens Advice**

Network of centres offering free, confidential and independent advice.

In England, call Adviceline: **0800 144 8848**In Wales, call Advicelink: **0800 702 2020** 

For online information and to find your nearest Citizens Advice:

In England: www.citizensadvice.org.uk
In Wales: www.citizensadvice.org.uk/wales

### **Citizens Advice Consumer Service**

Provides information and advice on consumer issues by telephone and online. Offers tips on avoiding scams.

Tel: 0808 223 1133

Welsh-speaking adviser: 0808 223 1144

In Northern Ireland, contact Consumerline

Tel: 0300 123 6262

### **Financial Conduct Authority (FCA)**

Provides advice on choosing a financial adviser. There's a scam warning tool for checking if an investment offer might be a fraud and a register for checking whether a company is authorised by the FCA.

Tel: **0800 111 6768** www.fca.org.uk

ScamSmart Investment checker: www.fca.org.uk/scamsmart

Financial services register: register.fca.org.uk/s/

### **Financial Ombudsman Service**

You can escalate complaints using this service if you're not satisfied with how your bank or building society has treated you after you've reported a scam.

Tel: 0800 023 4567

www.financial-ombudsman.org.uk

### **Friends Against Scams**

Offers information and advice and the Scam Marshals scheme.

www.friendsagainstscams.org.uk

### **Get Safe Online**

Gives free advice and tips on using the internet securely.

www.getsafeonline.org

### **GOV.UK**

Provides information about services and support, with advice on crime prevention and the Tell Us Once service.

www.gov.uk

www.gov.uk/find-local-trading-standards-office

### **Law Society of Northern Ireland**

Contact them to check if a solicitor is registered in Northern Ireland.

Tel: 028 9023 1614 www.lawsoc-ni.org

### **Mailing Preference Service (MPS)**

Free register for individuals who don't want to receive unsolicited sales and marketing contacts by post.

Tel: 0207 291 3310 www.mpsonline.org.uk

### **Metropolitan Police**

Contact them for specialist scams publications and advice.

Tel: 101 (non-emergency) www.met.police.uk

To find your local police service, visit www.police.uk/pu/your-area

### MoneyHelper

Gives impartial information about financial products and services and offers tips on everyday money management. Its Pension Wise service offers guidance about your pension.

Pensions Helpline: **0800 011 3797** Money Adviceline: **0800 138 7777** 

www.moneyhelper.org.uk

### **National Cyber Security Centre**

Provides information and advice about staying safe online.

www.ncsc.gov.uk

### **Personal Finance Society**

Can help you understand what financial choices you have and allows you to search for a qualified financial adviser.

Tel: **020 8530 0852** www.thepfs.org

### **Royal Mail**

Takes reports of scam mail. Either email them or post your letter directly to FREEPOST SCAM MAIL.

Tel: 0800 011 3466

Email: scam.mail@royalmail.com

www.royalmail.com

### **Solicitors Regulation Authority**

Regulates solicitors and law firms across England and Wales. You can check if a law firm or individual solicitor is registered with them.

Tel: **0370 606 2555** www.sra.org.uk

### **Telephone Preference Service (TPS)**

Free opt-out service for individuals who don't want to receive unsolicited sales and marketing telephone calls.

Tel: 0345 070 0707 www.tpsonline.org.uk

### **Think Jessica**

Campaign against scam mail. Includes stories of scam mail victims, along with resources for help and advice.

www.thinkjessica.com

### **TrustMark**

Organisation that helps you to find a trustworthy tradesperson.

Tel: 0333 555 1234 www.trustmark.org.uk

### **Unbiased**

List of qualified, independent financial advisers in your area.

Tel: 0800 011 9671 www.unbigsed.co.uk

### **Victim Support**

Provides free and confidential help to victims and witnesses of crime in England and Wales.

Tel: 08 08 16 89 111

www.victimsupport.org.uk

In Northern Ireland, contact Victim Support NI

Tel: 02890 243133

www.victimsupportni.com

### Help us be there for someone else

We hope you found this guide useful. When times are tough, it's so important to get some support. You can help us reach everyone who needs us:

- Tell us your story. If Age UK's information and advice has helped you, we'd love to hear about it. Email stories@ageuk.org.uk.
- Donate to us. We rely on donations to support older people when they need us most. To make a donation, call us on 0800 169 8787 or go online at www.ageuk.org.uk/donate.
- Volunteer with us. Our volunteers make an incredible difference to people's lives. Find out more at www.ageuk.org.uk/volunteer or contact your local Age UK.
- Campaign with us. We campaign to make life better for older people, and rely on the help of our strong network of campaigners. Add your voice at www.ageuk.org.uk/campaigns.
- Remember us in your will. A gift to Age UK in your will is a very special way of helping older people get expert support in the years to come. Find out more by calling 020 3033 1421 or visit www.ageuk.org.uk/legacy.

### What should I do now?

You might want to read some of our relevant information guides and factsheets, such as:

- Staying safe
- Looking after your money
- Advice for carers

You can find all of our guides and factsheets on our website, along with lots more useful information. Visit **www.ageuk.org.uk** to get started.

You can order free printed copies of any guide or factsheet by emailing **orders@ageuk.org.uk** or calling our Advice Line on **0800 169 65 65.** Our friendly advisers can also help with any questions.

All of our publications are available on request in large print and audio formats.

If contact details for your local Age UK are not in the below box, call Age UK Advice free on **0800 169 65 65**.



0800 169 65 65 www.ageuk.org.uk









Age UK is a charitable company limited by guarantee and registered in England and Wales (registered charity number 1128267 and registered company number 6825798). Registered address: Age UK, 7th Floor, One America Square, 17 Crosswall, London EC3N 2LB. Age UK and its subsidiary companies and charities form the Age UK Group. ID205694 08/25