Scamwise
Spotting, avoiding and reporting scams
Thank you
Independent Age would like to thank those who shared their experiences as this guide was being developed, and those who reviewed the information for us.

What do you think?
We welcome your feedback on our publications. We will use your comments to help us plan future changes. If you would like to help us to develop our information products, you can join our Readers’ Panel. For more information visit independentage.org/readers-panel or call 0800 319 6789.

Other formats
If you need this information in a different format (such as large print or audio CD), please contact us.

Contact us
Call us on 0800 319 6789 or email advice@independentage.org

Our publications cover England only. While we make every reasonable effort to ensure that our information is accurate at the time of publication, information can change over time. Our information should not be used as a substitute for professional advice. Independent Age does not accept any liability for any loss, however caused, arising from the use of the information within this publication. Please note that the inclusion of other organisations does not constitute an endorsement from us.

The sources used to create this publication are available on request.
About this guide

Scams are crimes. They are fraudulent tricks, designed to deceive you into giving away your money, possessions or personal details. Any of us can fall for a scam and they’re a growing problem, so it’s important to be aware of where you might encounter them. You can arm yourself against most scams with a few simple precautions, and if you’ve been the victim of a scam there are places you can find help.

If you have been scammed, it’s important to remember it isn’t your fault and you have nothing to feel ashamed of. Scams can be very sophisticated and many people are taken in – you have been the victim of a crime.

We spoke to older people about their experiences. Their quotes appear throughout.
Avoiding and spotting scams

Tips on spotting scams

One of the best ways to protect yourself is to arm yourself with knowledge about what a scam might look like. Scams often share some common features, which can help you to recognise them.

It may be a scam if:

1. **You’re contacted out of the blue** – for example, you receive an unexpected message from a person or company you’ve never heard of, or from what seems to be a familiar company but asking for something unlikely.

2. **You’re told to take urgent action** – tight deadlines and ‘make sure you don’t miss out’-type language are designed to pile on the pressure and stop you from thinking clearly. Scammers might try to make you panic by suggesting you’ll be at risk legally or financially if you delay.
3. What it says is unlikely – if it sounds too good to be true, it probably is. For example, you might be told you’ve won a prize draw you don’t remember entering, or be offered an investment opportunity with returns that sound improbably good.

4. You’re told to keep it secret – be suspicious if you’re asked not to tell anyone else, or told not to ring an organisation like your bank to check what you’re being told is accurate. This can stop you sharing information with other people who might notice something suspicious.

5. The communication is unprofessional – bad spelling and grammar, and overly familiar or odd language, are common in scams. This is a deliberate tactic to target the most vulnerable people, who might not notice these errors. Scam communications might use vague or unlikely-looking contact details, such as a mobile phone number, a PO Box, or an email address that’s different to what you would expect.

6. You’re asked to pay money upfront – for example, for goods or services that won’t materialise, to release a non-existent prize they claim you’ve won, or to claim a non-existent inheritance.
7. You’re asked for personal or banking information – for example, your passwords, bank account information, four-digit bank card PIN, or National Insurance number.

A communication doesn’t need to tick all of these boxes to be a scam – for example, some may look very professional and genuine.

To test your scam-spotting skills, try our online quiz (independantage.org/scams-quiz).
Security dos and don’ts

Scams can come in many forms. Here are a few places you might come across them and ways to guard yourself against them.

Door-to-door

Door-to-door scammers may try to sell you non-existent or poor-quality goods or services.

Do

 ✓ ask for identification before letting anyone in
 ✓ check credentials – eg their business address at [gov.uk/get-information-about-a-company](https://gov.uk/get-information-about-a-company) – before purchasing anything
 ✓ get personal recommendations when looking for reputable traders, or search for one through Trustmark ([0333 555 1234, trustmark.org.uk](https://trustmark.org.uk))
 ✓ get at least two quotes from traders for anything like building work, and get a written contract before work begins
 ✓ put up a ‘no cold callers’ sign to deter people
 ✓ consider getting a chain on your door or fitting a door viewer
✓ check other entrances are secured before answering the door, as door-to-door callers can also try to distract you while someone else enters your home to burgle you.

Don’t

✗ be pressured into buying anything on the spot – ask for time to consider and shop around to check the price you’ve been quoted is fair
✗ pay for any work, such as home maintenance or window cleaning, until it’s been completed and you’re happy with it
✗ ring a phone number on their ID card to check who they are – look up the company in the phone book instead.

It’s important to know if door-to-door callers are legitimate. As a social worker, I have to visit people regularly. I always call the person and their family before I visit, and I give my contact number and describe my appearance so they can check it’s a legitimate visit.
Cash machines

ATM fraud is rare, but it’s important to be alert at cash machines, as scammers can try to get your bank card or card details.

Do

✔ cover the keypad – eg with your hand – when entering your PIN. Scammers can peer over your shoulder or use hidden cameras to read your PIN

✔ check your accounts regularly and report any suspicious withdrawals

✔ if your card gets swallowed, report it to your bank immediately. Don’t leave the machine to make the call if possible – scammers can install devices to trap your card and then retrieve it when you’ve left

✔ keep your bank’s phone number with you in case of emergencies, for example in your phone

✔ use cash machines in banks, which may be less vulnerable to being tampered with than those on the street.
Don’t

✖ tell anyone your PIN
✖ let people distract you while you use an ATM or use it if people are lingering there
✖ use an ATM if there are signs it’s been tampered with – eg a loose keypad or wobbly card slot.
Internet

Scammers can use the internet to con you out of money and personal details, or to install harmful programs on your computer.

Do

✔ create strong passwords and change them regularly. Stringing together three random words can create a strong but memorable password. You can also use a mix of letters, numbers and symbols

✔ install antivirus software and update it when prompted

✔ keep your browser – eg Firefox, Chrome, Internet Explorer – and computer operating system up to date. You’ll usually be prompted to do this

✔ if you’re using social media, check your privacy settings to make sure you’re only sharing information you want to. Review the settings regularly – they can change when software is updated.

Don’t

✗ buy anything through an unsecured website. If the page is secure, there should be a padlock in the browser bar and the website name should start with ‘https:’ not ‘http:’ – the ‘s’ means secure
give someone access to your computer if they ring claiming there’s a problem with the computer, which they need to fix. Hang up if you get a call claiming to be from technical support

use public wi-fi to transmit personal data – eg don’t use it for internet banking or email. Only do financial transactions – shopping or banking – online when you’re at home or staying with a friend whose internet connection you trust.

Visit getsafeonline.org for more tips.

Like everyone else, I get frequent calls from 'Windows technical department', or about amazing investment opportunities. I have caller display, so for the majority I can see the origin of the call is overseas.
Email

Emails from spammers are often used to fish for your personal information, for example your bank details or passwords. This is known as phishing. They might also contain viruses that can slow down your computer or destroy files.

Do

✔️ use an email account that filters spam and keep the filter switched on
✔️ contact your bank immediately if you’ve been tricked into revealing any bank details
✔️ report scam emails to Action Fraud (0300 123 2040, actionfraud.police.uk/scam-emails) even if you haven’t fallen victim to them – it can help police to catch the scammers. If you have fallen victim to a scam, see chapter 5.

Don’t

✖️ open suspicious emails – eg from an unknown sender, or with a misspelt company name or subject line
✖️ open links or attachments in emails from someone you don’t know
✖️ respond to requests for money or for your personal or financial details
- click on links in suspicious-looking emails, even to unsubscribe. If an email asks you to change details in an online account, go to the account via the website
- reply to hard luck stories from unknown senders. Be aware that if you get an email from a friend with a tragic story asking for money, their email account may have been hacked. Contact them by other means to check whether it’s true.

Phone

Scams that try to trick people via a phone call are on the rise, and are often targeted at older people. In chapter 4, we look at some of the common techniques they use. Here are a few general tips to protect yourself:

Do

- hang up on cold callers and ignore cold texts
- sign up with the Telephone Preference Service to opt out of receiving unwanted sales and marketing calls (0345 070 0707, tpsonline.org.uk)
- see if your home phone or mobile phone has an option to block unwanted calls or texts
✓ remember, if you have a smartphone, it acts like a mini computer, so keep its operating system up-to-date and install antivirus software. Only download apps from official app stores, as apps can infect your phone with viruses. As with emails, don’t click on links in unsolicited text messages.

Don’t

✗ ever give out bank details such as your PIN or online banking login details, including by keying your PIN into the phone

✗ assume a call is safe just because the number matches the number on your bank card or statement. Callers can modify the caller ID so that your phone displays a fake number

✗ make a decision about an investment based on what someone has told you over the phone. Always seek independent financial advice

✗ ring a number the caller gives you to check the legitimacy of a call. Use a source you trust to find the number – for example, the company’s website or the phone book.
Postal scams are different from junk mail – scams are trying to trick you out of your money while junk mail is just post you haven’t requested, usually advertising something. However, it can be hard to tell the difference, so reducing junk mail can also help protect you against postal scams.

Do

✔ register with the Mailing Preference Service to be taken off UK direct mailing lists (020 7291 3310, mpsonline.org.uk)

✔ watch out for unlikely stories – eg stories about an unclaimed inheritance, or investment opportunities that sound too good to be true

✔ shred post containing your personal details before throwing it away.

Don’t

✖ respond to unsolicited post – eg saying you’ve won a lottery you didn’t enter

✖ send money up front in return for something – eg to claim a prize – and treat any post asking for money with suspicion

✖ send personal or financial details to anyone.
You can use the tips in chapter 1 to help you spot a scam. If you’ve received any sort of communication that you think might be suspicious, don’t respond and don’t reveal any of your personal details. You can check online to find information about scams that regulators are already aware of. For example, the Financial Conduct Authority helps to protect people against investment scams by letting you check whether the person who contacted you is on their warning list (scamsmart.fca.org.uk). They also have a list of unauthorised firms to avoid doing business with (0800 111 6768, fca.org.uk/consumers/avoid-scams-unauthorised-firms). Action Fraud has a lot of information on different types of fraud (actionfraud.police.uk/a-z_of_fraud) or you can call them for advice (0300 123 2040).

Scams target vulnerable people, so you can also help by looking out for people you know – see chapter 6.
Who is targeted by scammers?

Anyone can become the victim of a scam – they target people of all ages, backgrounds and income levels. However, older people might be more susceptible as some scams often target people who live alone, are at home during the day, are willing to talk to the scammers, and might be more likely to have savings and valuables.

Certain types of scam might be more targeted at older people. For example, studies found that 80% of phone scam victims were over 55 and 65% of doorstep scam victims were over 75.

If you think a communication is fraudulent, don’t reply in any way, even to be removed from a mailing list. Scammers keep lists of people who reply to them, so you could then be targeted in future.
Lucy, Independent Age
Bogus traders target homes where they think someone susceptible to scams might live, and will use the appearance of the property to judge this – for example, they may look for homes with unkempt gardens, buildings in a state of disrepair, or obvious adaptations for elderly or disabled people such as grab rails.

The introduction of new pension freedoms has also led to over-55s being targeted with investment scams – see chapter 4 for more information.

Try not to worry about whether you’re likely to be targeted – the best thing to do is be aware of the tactics scammers use and protect yourself.

A woman came to the door claiming to be collecting for a charity for the blind. I was suspicious, so I didn’t give her anything. When I refused to make a donation, she tried to push past me into my house, but I managed to stop her. The police told me they’d dealt with 20 other cases like this in the area, and I’d been right not to trust her because the charity had confirmed she didn’t work for them.
Types of scam

Some common phone scam techniques

Phone scams are on the rise and scammers use a range of techniques. Here are a few common ones:

Vishing (voice fishing)

The caller poses as someone from a reputable organisation, such as your bank, in order to get you to reveal personal details or hand over money. You may also get text messages to your mobile phone asking for these details.

Protect yourself

• Don’t give out personal or financial details.

• Hang up and contact the organisation yourself – but also see the ‘No hang-up phone scam’ on page 20. Make sure you find the number yourself rather than use one you were given by the caller.

• Don’t transfer money from your account to another account, even if the caller says it’s to protect your money or the new account is in your name.
No hang-up phone scam

The scammers ring posing as someone from a reputable organisation, then tell you to call the organisation (eg your bank) to verify what they’re saying and give them your personal details. The scammer will pretend to hang up while you do this, but they’ll keep the line open – you’ll think you have got through to the organisation but you’ll still be talking to one of the scammers. They can use fake dialling tones so you don’t notice anything is wrong.

Protect yourself

- Don’t assume a caller is genuine.
- Use a different phone, wait 20 minutes, or ring a number you trust (eg your mobile) before ringing the organisation, to check the line is clear.

Missed call

Scammers may use automated systems to dial numbers very briefly, leaving a missed call on your phone. Calls are often from numbers starting 070 or 076. They might look like mobile phone numbers but are actually premium rate numbers and if you call back, you’ll be charged a high rate for making the call.
Scammers also send text messages to mobile phones that seem like they’re from an ordinary individual trying to contact their friend. If you call or text them back to let them know they have the wrong number, you’ll be charged a high rate.

**Protect yourself**

- Contact the Phone-paid Services Authority (0300 303 0020, psauthority.org.uk) if this happens to you.
- If you weren’t expecting a call and don’t recognise the number, don’t call back.

**Investment scams**

Scammers cold-call people to offer fraudulent investment opportunities. They may claim to be from a reputable investment company, or they may have details such as information about previous investments you’ve made, which you might think only a reputable company could have. If you invest once, they might target you again to invest more.

Since April 2015, people have been able to access their pension savings when they reach 55. Scammers are now targeting this age group and trying to con them out of their pension money. They might try to persuade you to put money into a fraudulent investment offering high returns.
Protect yourself

- Always seek independent financial advice before making an investment. You can find an adviser through the Society of Later Life Advisers (0333 2020 454, societyoflaterlifeadvisers.co.uk) or Unbiased (0800 023 6868, unbiased.co.uk).

- Check with the Financial Conduct Authority (0800 111 6768, scamsmart.fca.org.uk) to see if a company is registered – don’t rely on data from Companies House.

- The Pensions Regulator website has information about protecting yourself from pension scams (pension-scams.com), or call the Pensions Advisory Service for advice if you’re unsure about an offer you’ve received (0300 123 1047).

Be suspicious of all ‘too good to be true’ offers and deals. There are no guaranteed get-rich-quick schemes.

Jim, Metropolitan Police
Courier fraud

Scammers call you, saying they’re from an organisation such as the bank, police, or fraud investigators, and that there’s been fraudulent activity on your bank card. This may involve a no hang-up scam where you seem to be verifying it’s genuine – see ‘No hang-up phone scam’ on page 20. You’ll be asked to tell them your PIN or key it into the phone and a courier will then be sent to pick up your card, allegedly so they can resolve the problem with your card. The scammers will then have your card and PIN and can use this to spend your money.

Protect yourself

• Never give anyone your PIN – your bank and the police will never ask for this.

• Never give your card or cheque book to anyone who comes to the door – your bank and the police will never come to your home to collect these.
Advance fee fraud

This involves getting you to pay a fee in advance for non-existent or not-as-advertised goods and services, or so that you can collect ‘winnings’. For example:

- job opportunities that ask for some sort of upfront fee when you respond
- lottery winnings that ask for your bank details to release the prize to you
- dating or romance fraud, where scammers form a relationship with you using a fake profile and then ask you for money to help them out, or for personal details to commit identity theft.

Make sure you’re clear about how your bank will communicate with you. If you’re suspicious about a phone call or email saying it’s from your bank, you can always ignore it and contact them on a number you know or visit your local branch to check it’s genuine.

Anna, Independent Age adviser
Identity theft is when someone uses your personal details - such as your name and date of birth - to impersonate you. For example, they might use your identity to open a bank account

• fraud recovery fraud – if you have been a victim of fraud, fraudsters may then target you again pretending to be an organisation that can help you to get your money back, but asking for a fee to do this.

Protect yourself

• Treat unexpected communications asking for money with suspicion, even if the amount of money requested is small.

• Don’t send money to someone you’ve only met online, no matter how much you feel you trust them.

Holiday fraud

This type of fraud is increasing. Scammers sell non-existent holidays or holiday add-ons. They’ll often encourage you to pay by direct bank transfer away from a main holiday booking site – perhaps by saying you’ll get a better deal if you book that way. You might only realise you’ve been a victim when you arrive at your destination and find the booking doesn’t exist.
Protect yourself

• Watch out for holidays advertised at an unbelievably low price.

• Use credit cards rather than direct bank transfers to book holidays.

• Check details elsewhere if you can – for example, a property may have its own website. Use an online map like Google maps to check that the address isn’t fake and the location is where you’d expect.

• See ‘Security dos and don’ts – internet’ for more on staying safe.

Door-to-door scams

These scams involve selling poor-quality goods or services, or ones that don’t materialise. For example:

• window cleaning or gardening services that ask for an upfront fee and then don’t deliver the service

• scammers posing as charities asking for donations

• overpriced or shoddy home maintenance

• electricity meter credit scams offering cut-price credit top-ups on electricity prepayment
meters. Scammers use cloned keys to illegally top up meters – once this is detected by the energy company, the customer will have to pay the energy company again.

**Protect yourself**

- Contact the Charity Commission (0844 248 2658, gov.uk/government/organisations/charity-commission) to check if a charity is genuine or contact specific charities to see if they’re collecting in your area.
- See ‘Security dos and don’ts – door to door’ for more on staying safe.

A few weeks ago, someone turned up on my doorstep. He asked whether I’d had a new meter fitted, and said if so, he’d need to check the work to ensure that it had been fitted correctly. I asked him for his identification to prove he was representing the power company, and told him I’d need to give them a call before allowing him into my home. He hurriedly left saying he didn’t have time to waste on people like me.
What to do if you’ve been scammed

If you’ve been scammed it can be very distressing, but don’t be embarrassed – you are the victim. It’s important to report it and get any support you might need.

If you think you may have put your personal or banking details at risk, contact your bank straight away and keep an eye on your bank statements and credit reports. You may have been scammed if:

- your bank or credit card statement includes items you didn’t purchase
- goods or services you’ve paid for don’t appear
- you get post about credit cards or bank accounts you haven’t set up
- something you don’t recognise appears on your credit report.
Who to report it to

Don’t be embarrassed about reporting a scam. Because the scammers are cunning and clever there is no shame in being deceived. By reporting it you will make it more difficult for them to deceive others.
Jim, Metropolitan Police

It’s important to report scams to make sure the police are aware of what has happened and can try to stop the scammers acting again.

If you’ve been the victim of a scam – ie if you’ve lost money or exposed your personal details – contact Action Fraud, the national fraud and cyber crime reporting centre (0300 123 2040, actionfraud.police.uk/report_fraud). To report a scam email that you were targeted by but didn’t fall victim to, use their separate reporting tool (actionfraud.police.uk/scam-emails).

If a crime is in progress and you need immediate assistance, call the police on 999.
You can also report certain scams to Trading Standards via Citizens Advice’s consumer helpline. They can use this information to try to catch the people responsible before they target anyone else (03454 04 05 06, citizensadvice.org.uk/consumer/get-more-help/report-to-trading-standards).

Trading Standards looks at cases where companies have broken the law or treated you unfairly. For example, they may have failed to carry out work on your home properly, or pressured you into buying something you didn’t want.

If you get a letter that you think is a scam, forward it, along with the envelope it arrived in, to Royal Mail at Freepost, Scam Mail, PO Box 797, Exeter, EX1 9UN. They also ask that you complete a Scam Mail Report (03456 113 413, royalmail.com/personal/help-and-support/what-can-I-do-about-scam-mail).

If you’ve been tricked into calling a premium-rate number, contact the Phone-paid Services Authority (0300 303 0020, psauthority.org.uk) – they regulate the goods and services charged to phone bills.

**Getting your money back**

You may or may not be able to get your money back when you’ve been scammed. You might have more protection if you’ve paid for something by
credit card. Contact your bank as soon as possible if there has been an unauthorised withdrawal from your account or you’ve been tricked into giving out your personal or banking information.

The Money Advice Service has more advice on getting your money back if you have been the victim of a scam or identity theft (moneyadviceservice.org.uk/en/articles/identity-theft-and-scams-what-you-are LIABLE-for).

Support for victims of scams

When you report a scam to Action Fraud, they will ask if they can pass your details to Victim Support, a national charity helping victims of crime. Victim Support will contact you to offer you emotional support and practical help. You can also contact them directly (0808 168 9111, victimsupport.org.uk/help-and-support). You might find it helpful to talk to family and friends as well, or you could call Samaritans for confidential emotional support on 116 123.

People often feel ashamed or embarrassed about becoming the victim of scammers, but anyone can be caught out. Scams are crimes and we’re all potential targets. Don’t blame yourself or let embarrassment prevent you from reporting a scam and getting the support you need.
If you think someone else has been scammed

Some people – such as those who are socially isolated or have dementia – are more at risk of being scammed, and people don’t always realise they’re being targeted.

You can help by looking out for:

• unusual amounts of post or unusual phone calls
• whether they’re secretive about their finances
• whether they seem to have a sudden lack of money
• whether they seem to be buying lots of goods, or having work done on their house, that they don’t need.

Try to raise the issue with them and help them to report a scam to Action Fraud (0300 123 2040, actionfraud.police.uk/report_fraud) if they want.

If you’re concerned about someone you know who might be vulnerable – for example, someone with dementia who you’re caring for – discuss your concerns with your local council’s adult social services department.
Remember...

1. Guard your personal and banking details carefully. Never give out security details, such as your PIN or internet banking password.

2. Don’t assume a communication is genuine. Don’t worry about seeming rude – if you’re worried or in doubt, you can always hang up the phone, or close the door on a doorstep caller.

3. Don’t sign up to anything on the spot or let anyone rush or pressure you. Give yourself time to think about decisions and check the accuracy of what you’re being told. Get independent advice before getting involved in an investment opportunity.

4. Trust your instincts – if it sounds too good to be true, it probably is.

5. Remember, you’re in control. Think carefully and don’t make a snap decision you’ll regret.

Take Five is a national campaign offering impartial advice on protecting yourself from financial fraud. Visit takefive-stopfraud.org.uk for more information.
Sonia’s story

My father-in-law was scammed by people posing as scratch card touts. He and my mother-in-law had saved for a holiday home in Spain to enjoy in their retirement. As they were passing through Alicante airport, they were approached by someone selling scratch cards for the National Lottery for one euro. They bought one. The following week we came to Spain and were stopped by the same people, and we too bought what looked like a legitimate ticket. The people had ID badges and high-vis labelled jackets – all very convincing.

A few weeks later we received a very unconvincing photocopied letter saying that we had won the Spanish lottery and needed to call a number to claim our prize. I knew straight away that it didn’t look right, but sadly my father-in-law thought it was real and rang the number. Then came the constant calls convincing him that he had won the jackpot and telling him to send funds to release the winnings. They hounded him for weeks and he lost just over £7,000.
They kept it a secret from the family because they wanted to surprise us with a cash sum each, but then as time went on and they had sent several amounts, they realised it was a scam. Eventually, they told us what they had done and how upset they felt because it had been so convincing. We contacted the police and reported the scam. Sadly, the police told us that the gang could be operating anywhere in the world and it was very unlikely they would be caught. We never recovered the money.
Our free advice guides

Our practical, jargon-free advice guides give you the information you need to get the most out of older age.

Advice for later life
Being winter wise
Care homes
Choosing where to live
Coping with bereavement
Dealing with depression
Getting help at home
How to find the right care home
If you’re feeling lonely
Moneywise
Staying in control when you’re older

To order your free advice guides, call 0800 319 6789 or visit independentage.org
The information in this guide applies to England only.

If you’re in Wales, contact Age Cymru (0800 022 3444, agecymru.org.uk) for information and advice.

In Scotland, contact Age Scotland (0800 12 44 222, agescotland.org.uk).

In Northern Ireland, contact Age NI (0808 808 7575, ageni.org).

We want the UK to be the best place to grow older and we have ambitious targets to increase the number of older people we help and the difference we make. We receive no state funding and rely on income from individuals, trusts and other sources to continue providing our services to hundreds of thousands of older people in need.

Visit independentage.org to make a secure online donation and find out about other ways to support us. Alternatively, you can call us on 020 7605 4223 or email supporters@independentage.org.
About Independent Age

Whatever happens as we get older, we all want to remain independent and live life on our own terms. That’s why, as well as offering regular friendly contact and a strong campaigning voice, Independent Age can provide you and your family with clear, free and impartial advice on the issues that matter: care and support, money and benefits, health and mobility.

A charity founded over 150 years ago, we’re independent so you can be.

For more information, visit our website independentage.org

Call us for information or to arrange free, impartial advice from an expert adviser. Lines are open 8am-8pm, Monday to Friday, and 9am-5pm, Saturday and Sunday. Freephone 0800 319 6789 or email advice@independentage.org

Independent Age is the operating name of the Royal United Kingdom Beneficent Association.
Registered charity number 210729 (England and Wales), SC047184 (Scotland).