



**Independent
Age**



Scamwise

**Spotting, avoiding
and reporting scams**



Thank you

We would like to thank those who shared their experiences as this guide was being developed, and those who reviewed it for us. Our thanks also go to those who provided support in the production of this guide.

What do you think?

We welcome your feedback on our publications. We use your comments to plan future changes.

If you'd like to help us develop our information products, you can join our Readers' Panel. To find out more, call **020 7050 6560** or visit **independentage.org/readers-panel**.

Our publications

In this guide you'll find references to our other free publications. To order them, call **0800 319 6789** or visit **independentage.org/publications**.

If you would like this information in a different format – such as large print or audio CD – call us on **0800 319 6789** or email **helpline@independentage.org**.

While we make every reasonable effort to ensure that our information is accurate at the time of publication, we do not accept any liability arising from its use. Our information should not be used as a substitute for professional advice. The inclusion of other organisations does not constitute an endorsement from us.

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

© Independent Age 2024

Author: Independent Age

Publisher: Independent Age

Design: Maria Brosnan

Photography: Leanne Benson cover, pp3, 7, 22, 25, 40, 44, 47;

Centre for Ageing Better pp6, 11, 52; Maria Brosnan pp27, 29, 43

Contents

About this guide	2
1. Spotting and avoiding scams	3
2. Security dos and don'ts	7
3. Who is targeted by scammers?	22
4. Scams to watch out for	25
5. What to do if you've been scammed	40
6. If you think someone else has been scammed	47
7. Useful contacts	49
8. Summary	51
Elizabeth's story	52

Date of publication: September 2024

Next review date: September 2026

We spoke to older people about their experiences. Their quotes appear throughout. We have changed the names of some of the interviewees who wished to be anonymous. Some of the images seen throughout this guide are posed by friends of Independent Age.

The PIF TICK is the UK-wide Quality Mark for Health Information.

About this guide

Scams are crimes. They are tricks designed to mislead 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 protect 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.

Scammers exploit uncertainty, like the cost-of-living crisis or Brexit. They also take advantage of new rules, especially around pensions and TV licences. Be alert for new scams.

If you have been scammed, remember that it isn't your fault. Scams can be very sophisticated, and lots of people are tricked by them – you have nothing to be embarrassed about. You have been the victim of a crime.



In this guide, you'll find references to our other free publications. You can order them by calling **0800 319 6789**, or by visiting **independentage.org/publications**.



1. Spotting and avoiding scams

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

1. Spotting and avoiding scams

Tips on spotting scams

It may be a scam if:

- **you're contacted out of the blue** – for example, you receive an unexpected message from a person or company you've never heard of. It might also be a message from what seems to be a familiar person or company but they are asking for something unlikely
- **you're told to take urgent action** – tight deadlines and statements like 'make sure you don't miss out' 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
- **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 impossibly good
- **you're told to keep it secret** – be suspicious if you're asked not to tell anyone else about what is happening, or if you're told not to ring an organisation like your bank to check what you're being told is true. This can stop you sharing information with other people who might notice something suspicious

- **the communication is unprofessional** – bad spelling and grammar, and overly familiar or odd language, are common in scams. 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
- **you're asked to pay money upfront** – you should not have to pay large amounts of money upfront for goods or services, to release a prize or to claim an inheritance
- **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 at **independentage.org/scams-quiz**.

1. Spotting and avoiding scams

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





2. Security dos and don'ts

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

2. Security dos and don'ts

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 – anyone genuine should carry some form of ID.
- Take the time to check that they are who they say they are before buying anything. You can check their business address at **gov.uk/get-information-about-a-company**.
- Get personal recommendations when looking for good, trustworthy traders, or search for one through Trustmark (**0333 555 1234**, **trustmark.org.uk**).

“ It's important to know if door-to-door callers are genuine. 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.

- Get at least three written quotes from traders for anything like building work, and get a written contract before any work begins.
- Put up a 'no cold callers' sign.
- Think about getting a chain on your door or fitting a door viewer so you can see who you're answering the door to.
- Check other entrances are secured before answering the door. Some door-to-door callers will 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 – instead, look up the company online or visit your library and ask staff to look up the company's details.

2. Security dos and don'ts

Cash machines

ATM fraud is on the rise. It's important to be alert at cash machines, because scammers can try to get your bank card or card details.

Do

- Cover the keypad when entering your PIN. This could be with your spare hand, or a wallet or purse, for example. Scammers can peer over your shoulder or use hidden cameras to read your PIN.
- Check your accounts regularly and report any suspicious activity.
- If your card gets taken into the ATM and you can't get it out, report it to your bank immediately. If possible, don't leave the machine to make the call – scammers can install devices to trap your card and then retrieve it once you've left.
- Keep your bank's phone number with you in case of emergencies. You could save it as a contact in your phone, or write it down somewhere.
- Use cash machines inside banks where possible. They may be less likely to be 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 – like a loose keypad or wobbly card slot.



2. Security dos and don'ts

Internet

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

Do

- Create strong passwords and change them regularly. To create a memorable, strong password, string together three words and mix in numbers and symbols. For example, something like Car2Dog4Iris6@.
- Install legitimate antivirus software and update it when prompted.
- Keep your internet browser updated. Google Chrome, Firefox, Microsoft Edge and Safari usually update on their own when you close them.
- Update your computer's operating system regularly. It will usually update itself, or it might prompt you to do this through your computer settings. Do not update your computer from pop-ups that you don't recognise. Scammers can use pop-ups to hack your computer.
- Check your privacy settings if you're using social media, to make sure you're only sharing information with people 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:' instead of 'http:' – the 's' at the end means 'secure'.
- Give someone you don't know access to your computer, especially if they call saying they need to fix a problem with your computer. Hang up if you get a call claiming to be from technical support.
- Use public wi-fi to send personal data, such as for internet banking or email. If you are shopping or banking online, do this at home. If you do not have internet connection at home, use the internet at a friend or family member's home.
- Take part in online quizzes or surveys that ask for personal details, including dates of birth, maiden names or pet names. These things are commonly used as passwords.



To do

Visit **getsafeonline.org** or **independentage.org/get-advice/staying-safe/internet-safety** for more tips.

2. Security dos and don'ts

Email

Emails from scammers are often used to get your personal information, like 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

- Make sure the spam or junk filter on your email account is switched on.
- Contact your bank immediately if you think you've been tricked into revealing any bank details.
- Report scam emails to Action Fraud (**0300 123 2040**, **actionfraud.police.uk/report-phishing**) even if you haven't been tricked by them. It can help police to catch the scammers.

You can also forward the email to **report@phishing.gov.uk**, then delete it. Most banks and traders have an email address you can forward any spam to as well.

If you have fallen for a scam, see **chapter 5**.

Don't

- Open suspicious emails, like 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.
- 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 using the website.
- Respond to requests for money, or for your personal or financial details.
- 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, like a phone call, to check whether it's true.

“ 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. Rachael, Independent Age

2. Security dos and don'ts

Phone

Scams that try to trick people with 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, but 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**, www.tpsonline.org.uk).
- Contact your phone provider to see if it has the option to block unwanted calls or texts. Different providers have different call blocking and filtering products. Ask about getting a junk voicemail that can block phone numbers or types of call.
- Remember to keep the operating system on your smartphone up to date and install antivirus software. Only download apps from official app stores, because apps can be used to download viruses on to your phone.

Don't

- Ever give out your bank details, full card details or online banking login.
- Write your PIN down, on paper or in your phone.
- Assume a call is safe just because the number matches the number on your bank card or statement. Callers can change the caller ID so that your phone displays a fake number. If you get a call about your bank account, hang up. Then you can call the bank directly with the number on your card. If you can, use another phone to do this, or wait at least 20 minutes before calling.
- Make any decisions about investments based on what someone has told you over the phone. Always seek independent financial advice.
- Ring a number the caller gives you to check that a call is genuine. Use a source you trust to find the phone number – for example, a bank statement or letter, or the phone book (you can download a local directory at [bt.com/help/the-phone-book/a-z-directory-finder](https://www.bt.com/help/the-phone-book/a-z-directory-finder)). The same applies to websites – scammers can make fake websites with different contact information on them. So, if you're looking for a phone number online, double check that the website you're on is real.

2. Security dos and don'ts



Good to know

If you are looking for independent financial advice, always check that whoever is advising you is registered with the Financial Conduct Authority (**0800 111 6768**, **register.fca.org.uk**). All financial advisers in the UK have to be registered here.

“ Like everyone else, I get frequent calls from the ‘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.

Postal

Postal scams are different from junk mail. Junk mail is just post you haven't asked for, usually selling you something. But postal scams are trying to trick you into giving away money. They often look like lotteries or prize draws. 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**, **www.mpsonline.org.uk**).
- Watch out for unlikely stories – for example, stories about an unclaimed inheritance, or investment opportunities that sound too good to be true.
- Make sure you change your address on all mail you receive if you move house. Royal Mail also has a post redirection service. You will have to pay for this, but you can get a discount if you claim Pension Credit. Find out more at **royalmail.com/personal/receiving-mail/redirection**.
- Shred post containing your personal details before throwing it away. Also think about shredding anything with your address on it, like labels from parcels.

2. Security dos and don'ts

Don't

- Respond to unsolicited post.
- Send money up front in return for something – treat any post asking for money with suspicion.
- Send personal or financial details to anyone by post.

If you've received any sort of suspicious communication, don't respond and don't tell them any of your personal details.

Scams target vulnerable people, so you can also help by looking out for people you know – see **chapter 6**.

“ I have had letters stating that I'd won competitions I knew nothing about. I just shredded and binned them.



Good to know

The Financial Conduct Authority helps to protect people against investment scams by letting you check whether the person who contacted you is on its warning list (**0800 111 6768**, **fca.org.uk/scamsmart**). It also has a register of unauthorised firms to avoid doing business with (**register.fca.org.uk**).

Action Fraud has a lot of information on different types of fraud (**0300 123 2040**, **actionfraud.police.uk/a-z-of-fraud**).

Friends Against Scams is an initiative training people to protect themselves and others from scams (**friendsagainstscams.org.uk**). You could sign up online as one of its Scam Marshals.



3. Who is targeted by scammers?

Anyone can become the victim of a scam – scammers target people of all ages, backgrounds and income levels. But some older people are vulnerable because they are targeted more.

Scams often focus on people who:

- live alone
- are at home during the day
- are willing to talk to the scammers
- might be more likely to have savings and valuables.

Bogus traders target homes where they think someone vulnerable to scams might live, and will use the appearance of the property to judge this. They may look for homes with unkempt gardens, buildings in a state of disrepair, or obvious adaptations for older or disabled people, such as grab rails.

This shouldn't put you off getting home adaptations that you need. There are plenty of ways you can protect your home from scammers. For example, some councils give out 'no cold callers' signs you can put in your window. No legitimate sales people or charity workers will come up to your door if there is a 'no cold callers' sign. This way, you know to be suspicious of any strangers who do knock on your door.

3. Who is targeted by scammers?

“ 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. 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.

The introduction of 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.



4. Scams to watch out for

Here are some of the most common scams that you should look out for. This list doesn't have every scam on it, so always follow your instinct. If something doesn't feel right, it probably isn't right.

4. Scams to watch out for

Phone scams

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

Voice phishing

The caller pretends to be someone from an organisation you might recognise, such as your bank, to get you to reveal personal details or hand over money.

They might even ask you to hang up and call the organisation to verify what they're saying and give your personal details. The scammer will pretend to hang up while you do this, but they'll keep the line open. They can use fake dialling tones so you'll think you have got through to the organisation but you'll still be talking to one of the scammers. You may also get text messages asking for these details.

Protect yourself

- Don't give out personal or financial details over the phone.
- Hang up and contact the organisation yourself. Wait at least 20 minutes, and check the line is clear by calling a number you trust, or using a different phone (like a mobile phone).
- Don't transfer money from your account to another account, even if the caller says it's to protect your money or that the new account is in your name. A bank will never ask you to transfer money to a 'safe account'. A bank won't ask for your PIN.



4. Scams to watch out for

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. If you call back, you'll be charged a very high rate for making the call.

Scammers also send text messages to mobile phones that seem like they're from an ordinary person 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.

“ Make sure you're clear about how your bank will communicate with you.

Protect yourself

- Contact the Phone-paid Services Authority (**0300 303 0020**, psauthority.org.uk) if you have called back a scam call.
- If you weren't expecting a call and don't recognise the number, don't call back.



4. Scams to watch out for

Investment scams

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

It's now illegal for someone to cold call you about your pension so, if you are contacted in this way, it's probably a scam.

“ If you're suspicious about a phone call or email saying it's from your bank, you can always ignore it and contact it on a number you know or visit your local branch to check it's genuine.

Rachael, Independent Age

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](https://www.societyoflaterlifeadvisers.co.uk)) or Unbiased (**0800 023 6868**, [unbiased.co.uk](https://www.unbiased.co.uk)).
- Check with the Financial Conduct Authority (**0800 111 6768**, [fca.org.uk/scamsmart](https://www.fca.org.uk/scamsmart)) 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 ([thepensionsregulator.gov.uk/en/pension-scams](https://www.thepensionsregulator.gov.uk/en/pension-scams)), or contact the Money and Pensions Service if you're unsure about an offer you've received (**0800 011 3797**, [maps.org.uk](https://www.maps.org.uk)).
- Report unwanted calls about your pension to the Information Commissioners Office (**0303 123 1113**, [ico.org.uk/make-a-complaint](https://www.ico.org.uk/make-a-complaint)).

4. Scams to watch out for

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 be part of a no-hang-up scam where you seem to be verifying it's genuine – see voice phishing on **page 26**.

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 them 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 before you get non-existent or not-as-advertised goods and services, or so that you can collect a 'prize'.

Examples might include:

- 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
- 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.

4. Scams to watch out for

Holiday fraud

Scammers sell non-existent holidays, caravans and motorhomes, or holiday add-ons online.

They'll often encourage you to pay by direct bank transfer away from a secure site – perhaps by saying you'll get a better deal that way. You may receive 'confirmation' emails. You might only realise you've been a victim when you arrive at your destination and find the booking or vehicle doesn't exist.

Protect yourself

- Watch out for holidays advertised at an unbelievably low price.
- Always book through a travel agent you recognise. The Association of British Travel Agents (**020 3117 0599**, **abta.com**) has a register of reputable agents.
- Use credit cards rather than direct bank transfers to book holidays.
- Check details elsewhere. Search for reviews online to make sure the information is genuine.
- See **page 12** for more on staying safe.

Check the latest guidance at **takefive-stopfraud.org.uk/advice/general-advice/purchase-fraud/holiday-fraud**.

Door-to-door scams

These scams involve selling poor-quality goods or services, or ones that don't get delivered, such as:

- 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
- burglars posing as salespeople so that they can scope out your home to rob later
- fake consumer surveys.

“ A few weeks ago, someone turned up on my doorstep. He asked whether I'd had a new meter fitted. 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.

4. Scams to watch out for

Protect yourself

- Contact the Charity Commission (**0300 066 9197**, **gov.uk/charity-commission**) to check if a charity is genuine, or contact specific charities to see if they're collecting in your area.
- Remember that people collecting for charities must follow certain rules. They must be carrying a licence from the council. They have to wear an ID badge that you are able to see, and that is at least the size of a credit card. They cannot be in groups of more than two people. They are not allowed to make you feel uncomfortable or scared, and have to leave if you tell them to.
- See **page 8** for more on staying safe.
- Check that anyone selling door to door has a valid pedlar's certificate issued by the police. They must show you the certificate if you ask.

Identity scams

Identity theft is when someone uses your personal details to impersonate you. They often use other scams like phishing emails (**page 14**) to get your personal information. Scammers can then steal your identity once they know things like your date of birth, full name or address.

Identity fraud is when a criminal uses a stolen identity to commit fraud. They can open bank accounts, get credit cards, loans and state benefits, order goods in your name, or take over existing accounts.

Protect yourself

- Make sure you shred anything with your name, address or financial information on it, before throwing it away.
- Don't leave things like bills or bank statements lying around where people can see them.
- If your credit card is lost or stolen, call your bank to cancel it as soon as possible.
- Keep an eye on your bank statements to check for any unexpected costs.
- Be aware of how to protect yourself from scams that phish for information (see **pages 14** and **26**).

4. Scams to watch out for

Dating or romance fraud

Dating or romance fraud is where scammers form a relationship with you using a fake profile. They then ask you for money to help them out, or for personal details to commit identity theft. These scams may take a lot of time and be very emotional, because the scammers have to build a relationship with you.

Protect yourself

Be wary of someone who:

- asks a lot of questions but doesn't reveal much about themselves
- rushes to steer you away from the site where you met, and communicate by email, text or phone instead
- is very emotional, or tells you a hard luck story before asking you to send them money
- doesn't want to video call or meet in person
- asks you to keep the relationship secret.

If you haven't ever met in person, it's important that you don't:

- send them any money
- give them access to your bank account
- take out a loan for them
- give them a copy of your passport or driving licence
- buy them online gift cards
- take in or send any parcels for them.

“ The focus relating to scams and fraud should always be on the harm this crime has caused this individual. We need to build community resilience and increase knowledge to prevent this. Louise, National Trading Standards Scams Team



5. What to do if you've been scammed

Being scammed can be distressing, but there is nothing to be embarrassed about. You are the victim of a crime. It's important to report it and get the support you need.

If you think your banking details may be at risk, wait at least 20 minutes before contacting your bank using the number on the back of your card, or on your latest statement.

You should also 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 arrive or happen
- you get post about credit cards or bank accounts you haven't set up
- something you don't recognise appears on your credit report.

“ 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

5. What to do if you've been scammed

Who to report it to

It's important to report scams so that the police know what has happened and can try to stop the scammers acting again.

If you've lost money or exposed your personal details because of a scam, contact the following agencies:

- if you live in England and Wales, contact Action Fraud, the national fraud and cybercrime reporting centre (**0300 123 2040**, **actionfraud.police.uk/report_fraud**)
- if you live in Scotland, contact Police Scotland directly by calling **101**.

To report a scam email that you were targeted by but didn't fall victim to, forward it to the Suspicious Email Reporting Service (**report@phishing.gov.uk**).

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 by contacting Citizens Advice's consumer helpline (**0808 223 1133**, **[citizensadvice.org.uk/consumer/get-more-help/report-to-trading-standards](https://www.citizensadvice.org.uk/consumer/get-more-help/report-to-trading-standards)**).

Trading Standards can use this information to try to catch the people responsible before they target anyone else. It looks at cases where companies have broken the law or treated you unfairly – for example, if they have failed to carry out work on your home properly, or pressured you into buying something you didn't want.



5. What to do if you've been scammed

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**. Royal Mail also asks that you complete a Scam Mail Report (**0800 011 3466**, personal.help.royalmail.com/app/answers/detail/a_id/303/kw/scam).

If you've been tricked into calling a premium-rate number, contact the Phone-paid Services Authority (**0300 303 0020**, psauthority.org.uk). It regulates 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 a withdrawal from your account that you did not know about, or if you've been tricked into giving out your personal or banking information.



Good to know

The Money Advice Service has more advice on getting your money back if you have been the victim of a scam or identity theft (**0800 138 7777**, **moneyhelper.org.uk/en/everyday-money/credit/identity-theft-and-scams-what-you-are-liable-for**).

5. What to do if you've been scammed

Support for victims of scams

Falling for a scam might be very upsetting.

When you report a scam to Action Fraud, they will ask if it can pass your details to Victim Support, a national charity helping victims of crime.

Victim Support will contact you to offer you free emotional support and practical help. You can also contact them directly (**0808 168 9111**, **victimsupport.org.uk/help-and-support**). If you live in Scotland, contact Victim Support Scotland (**0800 160 1985**, **victimsupport.scot**). You could also talk to family and friends, or call Samaritans for confidential emotional support on **116 123**.

People often feel ashamed or embarrassed about being scammed, but anyone can be caught out. Scams are crimes and we're all potential targets. Don't blame yourself or let embarrassment stop you from getting the support you need.

“ Seeking help doesn't come naturally to many people in my generation and I have always been an independent spirit, but it is so important for people to know how the system works.



6. If you think someone else has been scammed

Some people are more at risk of being scammed, and people don't always realise they're being targeted.

6. If you think someone else has been scammed

Some people are more vulnerable because, for example, they are socially isolated or have dementia. You can help someone you know by looking out for:

- unusual amounts of post or unusual phone calls
- whether they have started being secretive about their finances
- whether they suddenly seem to have a lot less 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/reporting-fraud-and-cyber-crime**) if they want to.

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

7. Useful contacts

Action Fraud

National fraud and cybercrime reporting centre. Get in touch if you believe you've been scammed.

- **0300 123 2040**
- **actionfraud.police.uk/report-phishing**

Charity Commission

The regulator for charities in England and Wales. Contact it to check a charity is genuine.

- **0300 066 9197**
- **gov.uk/charity-commission**

Financial Conduct Authority

The Financial Conduct Authority (FCA) regulates and supervises businesses and firms across the UK. Always check that your financial adviser is registered with the FCA.

- **0800 111 6768**
- **fca.org.uk/scamsmart**



7. Useful contacts

Phone-paid Services Authority

Contact this UK regulator if you have been tricked into calling a premium-rate number.

- **0300 303 0020**
- **[psauthority.org.uk](https://www.psauthority.org.uk)**

Samaritans

- **116 123**
- **[samaritans.org](https://www.samaritans.org)**

Victim Support

This independent charity offers free emotional and practical support to anyone affected by a crime.

- **0808 168 9111**
- **[victimsupport.org.uk/help-and-support](https://www.victimsupport.org.uk/help-and-support)**

Victim Support Scotland

This independent charity offers free emotional support and practical help to anyone affected by a crime in Scotland.

- **0800 160 1985**
- **[victimsupport.scot](https://www.victimsupport.scot)**

8. Summary

- **Guard your personal and banking details carefully.** Never give out security details, such as your PIN or internet banking password.
- **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.
- **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 what you're being told. Get independent advice before getting involved in an investment opportunity. It's okay to say 'thank you, but no thank you'.
- **Trust your instincts.** If it sounds too good to be true, it probably is.
- **Remember, you're in control.** Think carefully and don't make a snap decision you'll regret.



Elizabeth's story

I usually screen my calls, but I was expecting a call so I picked up, even though I didn't recognise the number.

I received three calls in a row, which I think was a way to confuse me. The first call was about an online purchase I hadn't made using my debit card.

A minute later, I got a call from a 'police officer' who told me that someone had been arrested using my debit card.

And then someone claiming to be from the fraud department at my bank called me and told me that my savings had been withdrawn, then paid back in with counterfeit money, using my ID. I was told to speak to the 'police officer' again by pressing 999.

When the 'officer' told me there was an undercover operation going on and I should not speak to anyone for 48 hours if I wanted to get my money back, I knew it was a scam.

I put the phone down, waited a few minutes, then rang my bank, who reassured me that my money was safe.

I know about scams, but this whole situation caught me off guard and made me realise that it really can happen to anyone.

“ When the 'officer' said I should not speak to anyone for 48 hours if I wanted to get my money back, I knew it was a scam.

About Independent Age

No one should face financial hardship in later life.

Independent Age is the national charity focused on improving the lives of older people facing financial hardship. We offer free impartial advice and information on what matters most: money, housing and care.

We financially support local community organisations across the UK through our grants programme. We campaign for change for older people struggling with their finances.

You can call us on freephone **0800 319 6789** (Monday to Friday, 8.30am to 5.30pm) or email **helpline@independentage.org** to arrange to speak to one of our advisers.

To donate or help support our work, please visit **independentage.org/support-us**.



Independent Age
18 Avonmore Road
London
W14 8RR

charity@independentage.org
Helpline 0800 319 6789

independentage.org



© Independent Age 2024

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