

Avoiding scams



Who we are

Age Scotland is the national charity for older people. We work to improve the lives of everyone over the age of 50 so that they can love later life.

Our vision is a Scotland where everyone can love later life.

Our mission is to inspire, involve and empower older people in Scotland, and influence others, so that people can make the most of later life.

Our three strategic aims are to:



Help older people to be as well as they can be



Promote a positive view of ageing and later life



Tackle loneliness and isolation

How we can help

We know that growing older doesn't come with a manual. Later life can bring changes and opportunities to your life and you may need to know about rights, organisations and services which are unfamiliar to you.

That's why we provide free information and advice to help you on a range of topics including benefits and entitlements, social care, legal issues such as Power of Attorney, housing and much more. All of our guides are available to download for free from our website, or you can contact our helpline team to have copies posted to you for free.

The Age Scotland **helpline** is a free, confidential phone service for older people, their carers and families in Scotland looking for information and advice.

Later life can bring times when you just need someone to talk to. Our **friendship line** is part of our wider helpline and older people can call us for a chat. We're here to listen, provide friendship and offer support.

For information, advice and friendship



Call us free on: 0800 12 44 222
(Monday – Friday, 9am - 5pm)



Visit [agescotland.org.uk](https://www.agescotland.org.uk)
to find out more.



Contents

What is a scam?	1
Spotting a scam	1
Doorstep scams	2
Telephone scams	5
Mobile phone text scams	7
Mail scams	9
Online scams	11
Reporting a scam	13
Scams and dementia	15
Protecting yourself from scams	16
Further advice and information	17

400,000 older people living
in Scotland have been
targeted by scammers

What is a scam?

A scam - also known as a trick, con or swindle - is an illegal act of fraud with the sole purpose of getting money from you.

Anyone can fall for a scam, regardless of their age or health. However, older people can be at a greater risk of falling for a scam than younger people. Someone who lives alone and who has limited social contact may not be able to discuss a letter or a phone call they have received with someone else to work out if it is real or not.

People living with dementia can be at a higher risk of scams, as criminals may think that they will be easily confused, or not able to remember the details of what has happened.

Spotting a scam

Scams can come in many forms. This guide looks at doorstep scams, telephone scams, mobile phone text message scams, mail scams and online scams.

**Over £190 BILLION is lost
to acts of fraud per year**



Doorstep scams

Doorstep scams can happen when someone comes to your door and offers to carry out work, for example repairing your roof or driveway, or cutting back a tree. They may ask to read your electricity or gas meter without providing identification, tell you they are collecting on behalf of a charity or offer you a product at a fantastic price if you sign up immediately.

If you need repairs on your roof or driveway, or need help in your garden, your council may run a Trusted Trader scheme. Any trader or local business registered with the scheme will have been checked and approved by the council and is highly rated by customers. Contact your council to find out if a Trusted Trader scheme runs in your area.

A Care and Repair service may also be available locally. Care and Repair services operate in most areas of Scotland and offer independent advice and assistance to homeowners to repair, improve or adapt their homes so that they can live in comfort and safety.

Care and Repair can be particularly helpful if there are things around the house you can no longer manage to do yourself. The service is generally available to people who own their own homes, private tenants and crofters who are aged 60 or over and for those who have a disability.

They may have a handyperson scheme for minor tasks such as fitting a handrail or changing a lightbulb, or provide services such as fitting key safes and alarms. There may be a charge for these services.

For more information contact **Care and Repair Scotland** on **0141 221 9879** or see their website **www.careandrepairscotland.co.uk**.

What to look out for in doorstep scams:

- sellers who offer you a large discount or time limited offers and who try to bully or rush you into making an on the spot decision
- people who say they are charity collectors or meter readers, but cannot prove who they are and have no form of identification
- people who offer to drive you to the bank to get cash out, if you say you don't have any money to pay for the work they are offering
- people who say they are Police Officers and need to see your bank cards and PIN number.

What you can do:

- do not let them in - even if they seem polite and friendly, don't feel pressured into agreeing to anything or letting them into your home if you don't know them. If they are genuine, they won't mind you thinking about it and checking they are who they say they are first
- ask them to come back later when someone else can be with you. If the offer is genuine they will happily agree
- don't accept excuses for not showing identification. Meter readers and charity collectors always carry identification, and you can call the organisation they say they are from to check. Use a telephone number from the phone book or look it up online; don't use the number on their card or a number they give you
- if they won't go away contact the police on 101, or if you feel you are in danger, call the 999 emergency number
- put a 'no cold calling' sticker on or near your front door; you may be able to get one from your council's Trading Standards department, or you could buy or print your own.



Stop, lock, chain, check

Police Scotland offer the following simple advice to stop someone you don't know tricking their way into your home:

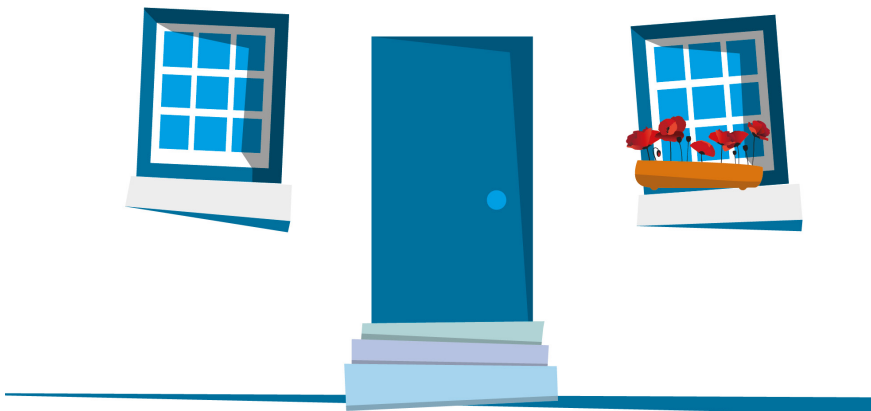
LOCK – Keep your front and back doors locked, even when you are at home.

STOP – Before you answer the door, stop and think if you are expecting anyone. Make sure your back door is locked, and you have taken the key out. Look through a spy hole or window to see who it is.

CHAIN – If you decide to open the door, put the chain or door bar on first if you have one. Keep the bar or chain on while you are talking to the person on the doorstep.

CHECK – Even if they have a pre-arranged appointment, check their identity card carefully. Close the door while you do this. If you are still unsure, look up a number in the phone book and ring to verify their identity. Do not use a phone number on the identity card as it may be fake.

IF YOU HAVE ANY DOUBTS, KEEP THEM OUT!



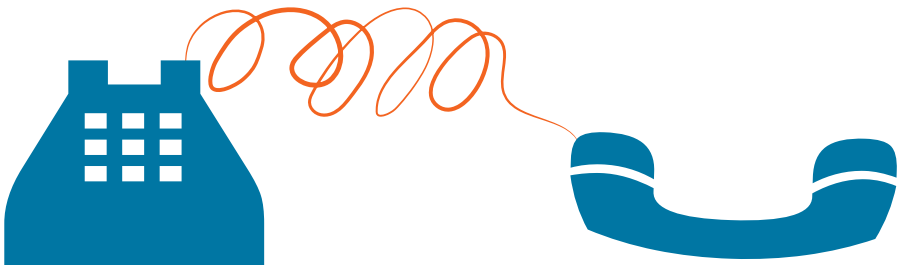
Telephone scams

Telephone scams usually involve someone trying to gain access to your bank account or computer.

What to look out for:

- calls from pushy salespeople offering large discounts or time-limited offers
- calls saying a subscription needs to be renewed and you have to pay straight away
- calls asking you to download something onto your computer, visit a particular website or give them remote access or passwords. They may say that your computer has a virus or has been hacked, and try to sell you software or offer to fix it for free
- calls to say you have won a prize
- calls asking for your personal information such as your name, date of birth, address and bank details.

If you think a phone call may be a scam, put the phone down immediately and report it to the police by calling 101.





What you can do:

- hang up - it is not rude to do this if you have any concerns that the call may be a scam
- never give out any personal information over the phone
- use caller identification tools or an answerphone to screen your calls, but still be careful as some scammers can now pretend to be calling from a number you know
- contact your telephone provider to make your number ex-directory, so it doesn't appear in the phone book
- even if the caller asks you to phone back on an official number so you can check they are genuine, make sure there is a dial tone before you call, so you know they haven't kept the line open after you hung up.

Call-blocking devices

These are devices that help you to manage nuisance calls. They usually let you choose trusted numbers, and block specific numbers or call types (for example calls from withheld numbers).

You can buy call-blocking devices online, or from some electrical and DIY stores and other retailers.

Telephone Preference Service

Signing up to the Telephone Preference Service will prevent UK companies that you don't already have dealings with from contacting you. Therefore, if you do receive a call, it is likely to be from a disreputable organisation and you will know not to trust them. Contact the **Telephone Preference Service** on **0345 070 0707** or visit **www.tpsonline.org.uk**.

Mobile phone text scams

These are often text messages giving you false information, with a link to click or a number to call. The message may sound urgent or alarming, to try to make you take action quickly without checking. For example, it may say there is a problem with your bank account or credit card, that you have been exposed to a health risk such as Covid-19, or even that there is a warrant out for your arrest. It may sound like it is from a friend or family member, asking for money urgently because they are in a difficult situation and giving you some account details to transfer funds to.

What to look out for:

- texts that say they are from your bank or other well-known organisation, that ask you to do something urgently
- texts that tell you to click on a link or call a number to update your details
- texts requesting personal information such as passwords or bank account details
- texts that say they are from one of your friends, but that come from a number you don't recognise or include a message that seems unusual or out-of-character.

What you can do:

- don't reply to the text message
- don't click on any links or call telephone numbers in the message
- contact your bank or other organisation on their advertised phone number, to check if the message is from them
- contact your friend on the number you hold for them to check if they sent you a message
- don't provide any personal information in response.



Mail scams

Scam mail may include advertising materials, junk mail and letters addressed directly to you. If you reply to these your details are likely to be shared with other companies, meaning you will receive even more unwanted mail.

What to look out for:

- letters saying you have won prizes such as money, cars, holidays or other luxury goods, in competitions you didn't enter, asking you to make a payment or call a premium-rate claim line
- letters from solicitors in other countries saying you have inherited money from a relative, and asking you to pay a release fee so the money can be sent to you
- letters telling hard-luck stories and asking for money to help with medical treatment or other expenses
- adverts for 'pyramid schemes' that ask you to pay a fee to join, then recruit friends or family members to join and pay fees too
- letters that ask you to invest money from your pension, with guarantees of large returns
- missed delivery notices that ask you to call a premium-rate number to arrange a redelivery.

What you can do:

- ignore any mail that you think is suspicious; throw it in the recycling bin after shredding or cutting up your name and address details
- never reply to mail that asks for money to claim a prize. Do not send money or give them any personal details
- do not phone any number on junk mail, as the call can cost up to £3.60 per minute¹
- register with the **Mail Preference Service** on **020 7291 3310**, a free service which can help to limit the amount of unwanted mail you receive
- speak to a reputable pension advisor before making decisions that may affect your pension, or contact Moneyhelper's **Pension Wise** advice service on **0800 138 3944**.



¹ www.gov.uk/call-charges

Online scams

Online scams are often emails asking you to visit a website and enter your password, bank details or other personal information. The website may even look exactly like the real one. This is sometimes called phishing.

They may also be ‘pop-up’ messages on websites telling you to click on them to claim a prize, or that your computer has a virus.

What to look out for:

- emails saying they are from your bank, telling you there is a problem with your account. They may ask you to go to a link contained in the email and put in your internet banking password
- emails telling you that you are owed a tax refund
- emails telling you that a direct debit has been declined, and asking you to visit a website to make a payment
- emails asking you to click links or download software onto your computer
- emails from well-known companies, but the email address looks different to their official one, or the email address looks normal but the contents of the email seem odd or unexpected
- emails from people you know, but saying things you wouldn't expect, such as ‘is this a video of you?’ with a link or email attachment
- poor spelling and strange formatting in official-sounding emails.



What you can do:

- keep online accounts secure by using strong passwords and keeping them to yourself - for advice about creating strong passwords, visit **Get Safe Online** at **www.getsafeonline.org/personal/articles/passwords**.
- consider using two-factor authentication to increase your level of security. This means you will use two different methods to verify your identity when you log into your email or other accounts. See **www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-2-step-verification-on-your-email** for information about two-factor authentication
- don't open email attachments from people you don't know
- don't click links in emails to access your accounts; always go to the official website to log in
- don't download software you don't trust
- if you think you have clicked on a link that may be fraudulent and have put in your account details, change your password immediately using the official website
- keep your antivirus software up-to-date and run a scan straight away if you think you have downloaded something from a source you don't trust
- visit **www.mygov.scot/staying-safe-online** to read the Scottish Government's advice about protecting yourself online, including ways to keep you, your family and your devices as safe as possible from scams and fraud
- for advice about protecting your devices, visit the **National Cyber Security Centre** at **www.ncsc.gov.uk/guidance/securing-your-devices**.

Reporting a scam

Some people feel embarrassed about being scammed and are reluctant to talk to friends, family, the police, their bank or other organisations.

However, being scammed can happen to anyone. The more quickly you report it the more easily something can be done about it. Reporting a scam could also prevent someone else from becoming a victim.

Police Scotland

If you are worried that a crime may have been committed or have a reason to be concerned, call 101 and speak to a local police officer.

Your bank or credit card provider

Call your bank or credit card provider immediately if you believe money has been taken or will be taken. The quicker you report it, the less likely you are to lose money.

Advice Direct Scotland

Contact Advice Direct Scotland for advice if you think you have been scammed. They can give you advice about what to do next, and can report the scam to Trading Standards if appropriate.

Tel: **0808 800 9060**

National Cyber Security Centre

If you have received a suspicious email, you can email it to the National Cyber Security Centre who have the power to investigate and remove scam email addresses and websites.

Email: **report@phishing.gov.uk**
www.ncsc.gov.uk



Royal Mail

You can report any scam mail that has been received in the post to the Royal Mail by telephone on or online. Scam mail can also be posted to Freepost Scam Mail.

Tel: **03456 113 413**
www.royalmail.com

Your mobile phone provider

Most UK mobile phone providers let you forward suspicious text messages to **7726** free of charge. They can investigate, and block or ban the sender if it is a scam message. The number 7726 spells SCAM on an alphanumeric keypad.

Financial Conduct Authority

Organisations offering pensions and investments must be authorised or registered with the Financial Conduct Authority. You can search their register online and can report unauthorised firms or individuals to them.

www.fca.org.uk

HMRC

You can forward suspicious emails and text messages to the HMRC's Phishing Team, or report details of suspicious calls to them by email.

Email: **phishing@hmrc.gov.uk**
Text: **60599**

If you think you have think you've given any personal information in reply to a suspicious email or text, email the HMRC security team. Give brief details but don't include personal information such as your address, HMRC user ID or password.

Email: **security.custcon@hmrc.gov.uk**

Scams and Dementia

Someone living with dementia can be seen as an easy target. Scammers may think that they will not be able to understand what they are being asked to do, remember the scam or describe what has happened. Depending on their mental capacity, they may not realise that they are doing something risky. They may also find it difficult to tell anyone what has happened in case they are not taken seriously.

If you are supporting someone living with dementia you can help to keep them safe by:

- helping them to get a call blocker
- looking at their post with them once a week and helping them to identify any scams
- set up antivirus software on a computer they use
- reinforcing the message that it is not rude to end an unexpected doorstep or phone conversation that makes them uncomfortable.

Protecting yourself from scams

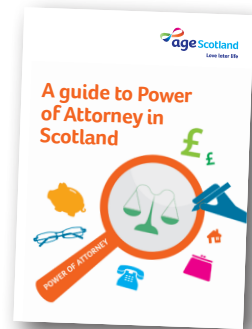
There are steps you can take to help protect yourself from scams:

- be suspicious – if someone contacts you in a way that seems odd, trust your instincts and check them out before you reply
- take your time – some scammers want to make you so anxious that you panic and can't think properly. Don't be rushed.
- get advice if you are not sure what to do. Call a friend, family or the Age Scotland helpline on **0800 12 44 222** and speak to an adviser about what's happening.

If you think someone is particularly at risk of scams, they may want to set up a Power of Attorney which would make someone they trust responsible for helping them look after their money.

For information see Age Scotland's guide to **Power of Attorney in Scotland**.

Or visit the website for **The Office of the Public Guardian (Scotland)**:
www.publicguardian-scotland.gov.uk
or call them on **01324 678398**.



Further advice and information

Age Scotland

The Age Scotland helpline provides information, friendship and advice to older people, their relatives and carers.

Tel: **0800 12 44 222**

Citizens Advice Bureau

You can call Scotland's Citizens Advice Helpline on **0800 028 1456** for advice or for details of your local bureau or see their website **www.citizensadvice.org.uk/scotland/about-us/get-advice-s/**

Victim Support Scotland

Support and advice for victims of crime in Scotland.

Tel: **0800 160 1985**

www.victimsupportsco.org.uk

How you can help

Our vision is a Scotland where everyone can love later life.

All the information and advice we provide is free and completely impartial and in helping people access their rights and entitlements, it can be life changing.

We are an ageing population and more people than ever are coming to us for support. You can help us be there for those that need us most.



Make a donation

No matter how small or large, donations make a massive difference and help us continue our important work.

- ▶ Call **03330 15 14 60**
- ▶ Visit **age.scot/donate**
- ▶ Text **LATERLIFE** to **70085** to donate £5.*



Fundraise

Whether it is having a bake sale, running a marathon or knitting small hats for the Big Knit, there are so many ways to raise vital funds to support our work. To find out more, call **0333 323 2400** or visit **age.scot/fundraise**.



Leave us a gift in your Will

By choosing to leave us a gift in your Will, you can help Age Scotland to continue being there for vulnerable older people in the years to come. To find out more, call **0333 323 2400** or visit **age.scot/legacy**.

* Texts cost £5 plus one standard rate message

Let's keep in touch



Sign up to our newsletter

Our regular newsletters by email contain details of our campaigns, services and how you can support our work.

Sign up today by visiting **age.scot/roundup**



Follow us on social media

Our social media channels are a great way to keep up to date with our work and issues that affect older people.



[/agescotland](https://www.facebook.com/agescotland)



[@AgeScotland](https://twitter.com/AgeScotland)



[@age_scotland](https://www.instagram.com/age_scotland)



[/AgeScotland](https://www.linkedin.com/company/AgeScotland)

Age Scotland is the national charity for older people. We work to improve the lives of everyone over the age of 50 so that they can love later life.

Our vision is a Scotland where everyone can love later life.

Contact us:

Head office

0333 323 2400

Age Scotland helpline

0800 12 44 222

Email

info@agescotland.org.uk

Visit our website

www.agescotland.org.uk

Follow us on social media:



/agescotland



@AgeScotland



@age_scotland



/AgeScotland



We are grateful to the
Scottish Government for
part-funding this publication

