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 and promote their rights and interests.

Our vision is a Scotland which is the best place in the world to grow older.

Our mission is to inspire, involve and empower older people in Scotland, and influence others, so that people enjoy better later lives.

We have three strategic aims:

We help older people to be as well as they can be

We promote a positive view of ageing and later life

We 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.

Our **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.

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

Visit agescotland.org.uk to find out more.

Contents

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.

People of all ages can fall for scams. However, older people can be at a greater risk from scams and of being targeted by scammers than younger people. Someone who lives alone and has limited social contact may not have anyone they can talk with to discuss a letter or phone call, to help them work out if it is real or not.

People living with dementia can be at an even higher risk from scams. Criminals may target people with dementia thinking 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 describes the main types of scams and what to look out for. It also tells you what you can do if you think you have been scammed.

Over £200 BILLION is lost to acts of fraud per year

Doorstep scams

Doorstep scams involve someone coming to your home and telling you to do something that would result in them getting money from you fraudulently. They may tell you they are from a trusted company, organisation or charity. They may even tell you they are a Police Officer.

Sometimes people come door-to-door offering to carry out repairs on your home or garden, but it is impossible to know who you can trust. Be wary of anyone who knocks on your door without an appointment.

Get trusted help

If you do need home repairs or help in your garden, ask your council if they run a Trusted Trader scheme. All registered traders will have been checked and approved by the council.

Care and Repair services also operate in most areas of Scotland. They are generally available to people aged 60 or over who are homeowners, private tenants or crofters, and for people with a disability. They offer independent advice and assistance to help people repair, improve or adapt their homes. They may have a handyperson scheme for jobs around the home such as changing light bulbs. They can also fit handrails, key safes and alarms. There may be a charge for these services.

Visit **www.careandrepairscotland.co.uk** for more information or call the **Age Scotland helpline** on **0800 12 44 222** for help finding the number for your local service.

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 instant 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. See page 7 for more information about scams that involve impersonating a Police Officer.

What you can do:

- Do not let them in - don't feel pressured into agreeing to anything or letting them into your home, even if they seem polite and friendly. If they are genuine, they won't mind you checking into who 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; a number on their card or that they give you may be fake.
- 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 advice to stop someone you don't know tricking their way into your home:

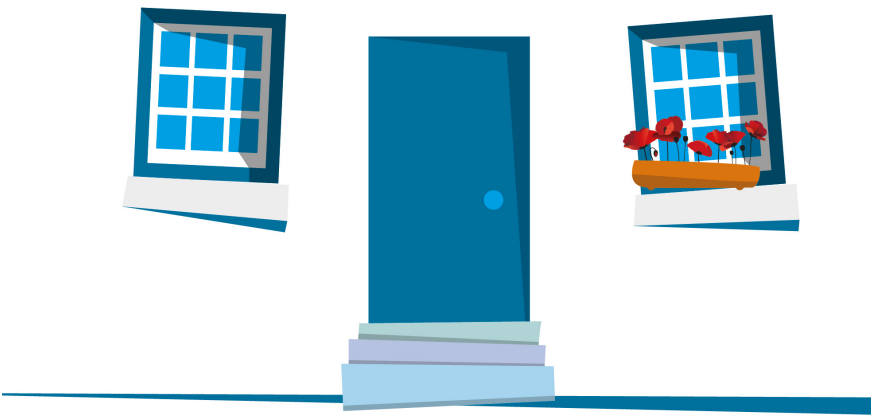
LOCK – Keep your front and back doors locked, even when you are at home.

STOP – Before you answer the door, stop and think whether 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!



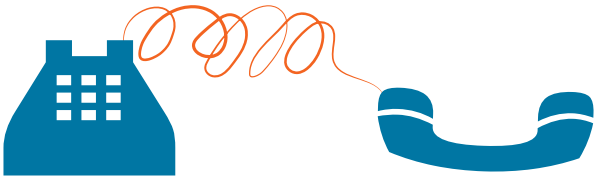
Telephone scams

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 from someone telling you they are from Police Scotland and they need you to do something urgently, or asking for personal details. See page 7 for more information about scams that involve impersonating a Police Officer.
- Calls asking you to download something onto your computer, visit a particular website or give the caller remote access or passwords. They may say your computer has a virus or has been hacked, and try to sell you software to fix it, or offer to fix it for free.
- Calls to say you have won a prize
- Calls asking for your personal information such as your full name, date of birth, address and bank details

If you think a phone call may be a scam, put the phone down immediately. Report it to the police by calling 101, preferably from a different phone if the call was to your landline. The caller could still be on the line if they have not hung up from their end. If you do not have another phone, make sure you can hear a dialling tone before making another call.



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
- Ask your telephone provider to make your number ex-directory, so it doesn't appear in the phone book
- If the caller invites you to phone back on an official number so you can check they are genuine, make sure there is a dialling 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 helps prevent UK companies you don't have dealings with from contacting you. Therefore, any unexpected calls you get are likely to be from disreputable organisations, and you will know not to trust them. Contact the **Telephone Preference Service** on **0345 070 0707** or visit **www.tpsonline.org.uk**.

Impersonating a police officer scams

Some criminals pretend to be police officers. They will tell you they have arrested someone caught using your bank card, or that they have identified suspicious activity on your bank account. You may be contacted by phone, in person as a doorstep scam, or by another method.

Part of the scam involves getting you to move money, which they will say is to protect it from being stolen from your bank account. If they have come to your home, ask to see their Police Scotland Warrant card. This should feature the Police Scotland logo, a hologram, and the signature of Chief Constable Iain Livingstone. If in doubt, call 101 to confirm they are a real police officer and that their visit is on record.

Police officers will never:

- Tell you to transfer money between bank accounts
- Ask you to make withdrawals of cash from a bank or ATM
- Tell you to go to a bank or post office to withdraw money, or offer to take you there themselves
- Ask for your PIN number or to see your bank cards

Text message 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, some messages may say there is a problem with your bank account or credit card, or even that there is a warrant out for your arrest. Others may appear to be from a friend or family member, asking for money urgently because they are in a difficult situation and providing account details to transfer funds to.

What to look out for:

- Texts that say they are from your bank or another well-known organisation, asking you to do something urgently
- Texts that tell you to click on a link or call a number to update your details or make an outstanding payment
- 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.
- Texts that say they are from a delivery company asking you to click a link to arrange a redelivery, or make an outstanding postage payment.

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 official 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
- If you think your number has been used to contact people you know, tell your contacts what has happened and warn them not to respond to any unusual messages that seem to be from you. You should also report this to the police by calling **101**.

Mail scams

Scam mail may come in the form of flyers, usually advertising schemes or deals, or as letters or notices 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 a prize in a competition you don't remember entering, asking you to make a payment or call a premium-rate claim line
- Letters from solicitors, particularly those in other countries, saying you have inherited money, 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 to recruit friends or family 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 you think is suspicious; shred it or cut up your name and address details before recycling it
- 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 calls can cost up to £3.60 per minute plus additional charges[1]
- Register with the **Mailing Preference Service** on **020 7291 3310** or **www.mpsonline.org.uk**, 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 the **MoneyHelper Pensions Helpline** on **0800 011 3797**
- You can report suspected scam mail to Royal Mail at **www.royalmail.com/reportingscammail** or send it to **Freepost Scam Mail**. You should include the envelope the scam mail was sent in and a Scam Mail Report, available at **www.royalmail.com**. You can also call **Advice Direct Scotland** on **0808 164 6000**.

[1] www.gov.uk/call-charges

Online scams

Online scams are often emails asking you to visit a website, usually by clicking a link in the email. You may be asked to enter your password, bank details or other personal information. The website may even look exactly like the real one. This is sometimes called phishing.

Some scams use 'pop-up' messages on websites. They might tell you to click on them to claim a prize, or that your computer has a virus and that you need to click to fix it.

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 that seem to be from well-known companies, but either the email address is different from the official one or the contents of the email seem odd or unexpected
- Emails from the email address of someone you know, asking for money or saying things you wouldn't expect, such as 'is this a video of you?' with a link or 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. **Get Safe Online**'s article explains more: **www.getsafeonline.org/personal/articles/two-factor-authentication**
- Don't open email attachments you weren't expecting to receive
- 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 that may not be trustworthy
- 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

Reporting a scam

Some people feel embarrassed about being scammed and are reluctant to report it or seek advice.

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

Police Scotland

If you are worried a crime may have been committed or have reason for concern, call 101 to speak to a local police officer. If you are reporting a phone scam, call using a different phone if the call was to a landline, or make sure you can hear a dialling tone before making the call.

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. You can call 159 to be connected to your bank if you cannot find the number.

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. Call **0808 164 6000** or report a scam online at **www.consumeradvice.scot**.

National Cyber Security Centre

If you have received a suspicious email, you can email it to the National Cyber Security Centre at **report@phishing.gov.uk**. They have the power to investigate and remove scam email addresses and websites. You can also forward scam texts to **7726** and report scam websites online at **www.ncsc.gov.uk**.

Royal Mail

Details of how to report scam mail can be found at **www.royalmail.com/reportingscammail**. The website also gives details of how to report suspicious emails, texts, calls or websites that say they are linked to Royal Mail. You can also report these by calling **Advice Direct Scotland** on **0808 164 6000**.

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.

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**

HM Revenue and Customs (HMRC)

Suspicious emails, calls, messages and websites related to HMRC can be reported to the HMRC phishing team. See details online at **www.gov.uk/report-suspicious-emails-websites-phishing** or call the **Age Scotland helpline** on **0800 12 44 222** for help finding the right contact details.

If you have given personal information in reply to a suspicious email or text, email **HMRC Security Team** at **security.custcon@hmrc.gov.uk**. Give brief details but don't include personal information such as your address, HMRC user ID or password.

Scams and Dementia

Someone living with dementia might be seen as an easy target for scams. Scammers may think the person will not understand they are being asked to do something risky. They may also assume the person will not remember the scam or be able to describe what happened, and that they will therefore be more likely to get away with it.

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

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

Protecting yourself from scams

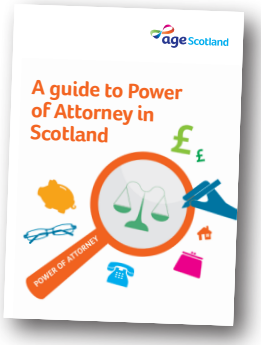
There are steps you can take to help protect yourself from scams:

- 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. Speak to a friend or family member, or call the Age Scotland helpline on **0800 12 44 222**.

If you think someone is particularly at risk of being scammed, you might like to encourage them to set up a Power of Attorney. This would enable them to give official permission to someone they trust to help them look after their money.

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

You can also visit the website for **The Office of the Public Guardian (Scotland)**: **www.publicguardian-scotland.gov.uk** or call them on **01324 678300** and choose option 1.



Who can help?

Age Scotland helpline 0800 12 44 222

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

If you need an interpreter call **0800 12 44 222** and simply state the language you need e.g. Polish or Urdu. Stay on the line for a few minutes and the Age Scotland helpline will do the rest.

You can call us on **0800 12 44 222** for a copy of our publications list. You can also download or order copies of our publications at **www.agescotland.org.uk**.

Police Scotland

You can visit the Police Scotland website at **www.scotland.police.uk** for advice and guidance about scams. You can also call 101 if it's not an emergency, to speak to a local police officer.

Citizens Advice Bureau

You can call Scotland's Citizens Advice Helpline on **0800 028 1456** for advice or details of your local bureau, or visit **www.cas.org.uk**.

Victim Support Scotland

Support and advice for victims of crime in Scotland.

Tel: **0800 160 1985**
www.victimsupport.scot

How you can help

Our vision is a Scotland which is the best place in the world to grow older.

All the information we provide is free and impartial. It helps older people access their rights and entitlements and can be life changing.

We are also a lifeline for older people who are feeling lonely and isolated. You can help us to support older people who need us most.

Together, we can make a difference.

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 **AGESCOTGIVE** to **70085** to donate £5*
- Complete the **donation form** and return by Freepost

Fundraise

Whether it's having a bake sale or running a marathon, 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 us to continue being there for 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

Please donate today

Complete the form and return to RSBS-KEHC-GBBC, Age Scotland, Edinburgh, EH9 1PR

Your details

Title: | Forename: | Surname:

Address:

City:

Postcode: | Date of birth:

By providing us with your telephone number and email address you are consenting to us contacting you via phone, text and email.

Email:

Home tel: | Mobile tel:

I WOULD LIKE TO DONATE

£75 ☐ £50 ☐ £25 ☐ Other (£) ☐

I wish to pay by (please tick):

MasterCard ☐ Visa ☐ CAF ☐

CharityCard ☐ Cheque ☐ (payable to Age Scotland)

Name on Card

Card No.

Expiry date | Security code

Signature | Date

I prefer not to receive a thank you acknowledgement for this donation ☐

I would like information about leaving a gift in my Will ☐

I WOULD LIKE TO MAKE MY DONATION WORTH 25% MORE

giftaid it

I want Age Scotland** and its partner charities to treat all donations I have made for the four years prior to this year, and all donations I make from the date of this declaration until I notify you otherwise, as Gift Aid donations.

I am a UK tax payer and understand that if I pay less income tax and/or capital gains tax than the amount of Gift Aid claimed on all my donations in that tax year it is my responsibility to pay any difference.

Yes, I want Age Scotland to claim Gift Aid on my donations** ☐

I do not wish you to claim Gift Aid on my donations ☐ **Date**

Keeping in touch

We will stay in contact by post unless you ask us not to. We will never sell your data and we promise to keep your details safe and secure. You can change your mind at any time by emailing us on contact@agescotland.org.uk or calling us on 0333 323 2400.

You can read Age Scotland's privacy policy at **age.scot/privacypolicy**.

**Age Scotland, part of the Age Network, is an independent charity dedicated to improving the later lives of everyone on the ageing journey, within a charitable company limited by guarantee and registered in Scotland.
Registration Number: 153343. Charity Number: SC010100. Registered Office: Causewayside House, 160 Causewayside, Edinburgh EH9 1PR.

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 which is the best place in the world to grow older.

Let's keep in touch

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

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 at **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.

POLICE SCOTLAND
POILEAS ALBA

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

The Scottish Government

We are grateful to the Greater Glasgow Police Division for their input to this guide.
Visit the Police Scotland website for advice and guidance at: **www.scotland.police.uk**
Tel: Dial **101** if it's not an emergency to speak to a local police officer
Facebook: /GreaterGlasgowPoliceDivision
Online contact form: **www.scotland.police.uk/secureforms/contact**

M13 Feb 2024