age Scotland
Love later life

Avoiding scams

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.

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.

Doorstep scams

Doorstep scams can happen when someone comes to your door and offers to repair your roof or driveway, or cut back a tree. They may also ask to read your electricity meter without providing identification, or offer you a product at a fantastic price.

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.

These 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.

These services may also run a handyperson scheme for minor tasks such as fitting a handrail or changing a lightbulb. There may be a charge for these services.

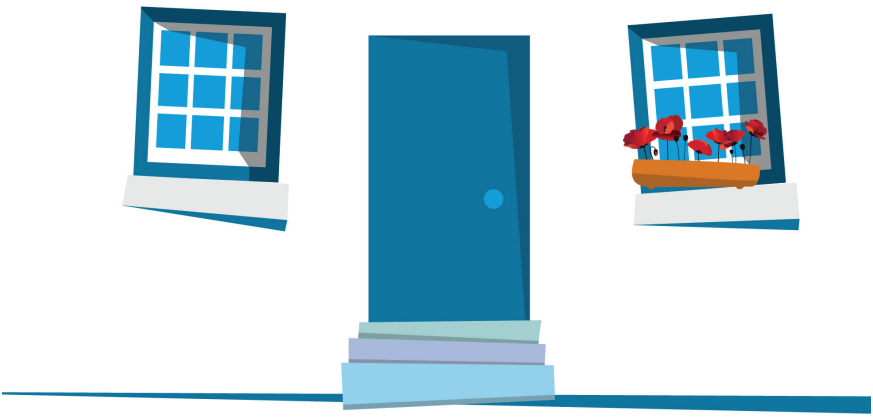
For more information contact **Care and Repair Scotland** on **0141 221 9879** or see their website **www.careandrepairscotland.co.uk**.

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 but cannot prove who they are and have no form of identification
- 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
- ask them to come back later when someone else can be with you. If the offer is genuine they will happily agree
- 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!

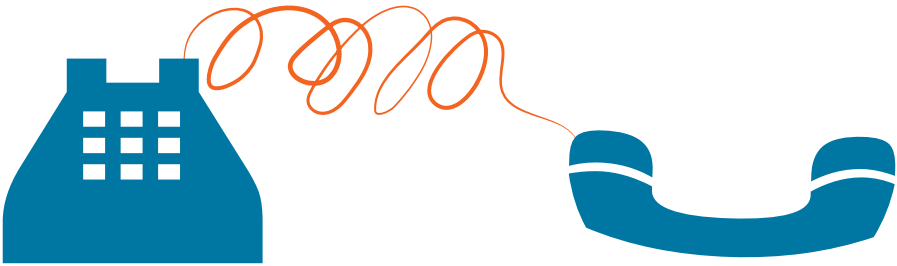
Telephone scams

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 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, immediately put the phone down 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
- contact your telephone provider to make your number ex-directory, so your number 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 may be able to get a call-blocking device free from **Trading Standards Scotland**. Visit **tsscot.co.uk/call-blocker-online-referral** to apply, or contact your council's Trading Standards department.

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 telling you there is a problem with, for example, you bank account, giving you a link to click on or number to call so you can fix it. The message may sound urgent or alarming, to try to make you take action quickly without checking.

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.

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 to a text message.

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 minute[1]
- Register with the **Mail Preference Service** on **020 7291 3310**. This free service should limit the amount of unwanted mail you receive
- Speak to a reputable pension advisor before making decisions that may affect your pension, or contact **Pension Wise** 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
- 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
- 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.

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**

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

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**

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

Online and face-to-face information and advice on a range of issues. Find your nearest bureau by searching on their website.

www.cas.org.uk/bureaux

Victim Support Scotland

Support and advice for victims of crime in Scotland.

Tel: **0800 160 1985**
www.victimsupportsco.org.uk

0333 323 2400
info@agescotland.org.uk
www.agescotland.org.uk

Age Scotland Helpline
0800 12 44 222

www.facebook.com/agescotland

www.twitter.com/agescotland

www.youtube.com/agescotland

M13 Apr 2020