Avoiding scams

Ways to protect yourself

AgeUKIG05

Information written with you in mind.

This information guide has been produced with the help of older people, carers and expert peer reviewers.

Published: **July 2023**

We'd love to hear from you.

1) Join our Readers' Panel. Have your say and be involved in updating our guides by joining our Readers' Panel. You don't need any specialist knowledge at all.

Join our Readers' Panel at **www.ageuk.org.uk/readers-panel**.

2) Tell us your story. Have you been affected by any of the issues in this guide? Has Age UK's information and advice helped? If so, we'd love to hear from you to provide relatable examples that benefit others.

Email your story to **stories@ageuk.org.uk**.

Contents

What this guide is about

Being scammed can be very distressing, and the impact is often emotional as well as financial – it can happen to any of us. If you've been scammed, you're not alone and there's support available.

This guide explains what you can do to protect yourself from scams and how to spot the warning signs that someone might be trying to scam you.

It explains:

- the ways scammers might try to approach you
- what you can do if you think you've been scammed
- how to avoid being scammed in the future.

As far as possible, the information given in this guide is applicable across the UK.

This symbol indicates where information differs for Wales and Northern Ireland.

What is a scam?

Scams are a way of cheating people out of their money – they're crimes. The people behind them are sometimes called fraudsters, swindlers or con artists. But in this guide, we refer to them as scammers or criminals.

You may be approached on your doorstep, by post, over the phone or online. New digital ways of communicating have led to an increasing number and variety of scams.

Any scam, even if you spot it in time, can leave you feeling shaken up and have a real impact on your confidence. But this guide can help you protect yourself by knowing what to look out for, and what to do if you suspect a scam.

What if someone I know is being scammed?

This guide is about protecting yourself against scams, but any tips you read here also apply to friends and family. If you're worried that someone you know is being scammed, you should:

- **look out for warning signs.** For example, the person may be getting unusually large amounts of post or spending a lot of money – or they may seem secretive or defensive about either of these things. It might help to give them some relevant advice from this guide (perhaps even share the guide with them) and encourage them to report the scam to the right organisation.
- **find support.** The charity Think Jessica (page 41) can help you support someone who doesn't believe they're being scammed. There are more useful organisations listed at the back of this guide too (pages 36-41).

The lasting impact of a scam

Often when we talk about scams, we discuss them in financial terms and don't talk about the emotional impact they can have. It's one of those things we just don't really talk about. But they can leave us feeling embarrassed, unsettled and unsafe and have a lasting impact on our confidence. They can also leave us feeling unsure about who we can trust.

But if you've been scammed, it's important to reach out and talk to people about what's happened. It's nothing to feel embarrassed about – these scams are increasingly sophisticated and are purposefully designed to steal your money by posing as people or organisations you trust. They can catch you on a day you're busy doing something else, or just having one of those days. We've all had them.

There's an element of pride and thinking that others might judge you or question your decision making, especially as you get older. But the truth is anyone can be scammed, and lots of people are scammed. By talking about it, you might be surprised by how many people you know are worried about scams too or have been scammed themselves.

The best way we can protect ourselves and others from scams is to speak about them. The more we know, the less effective they are, and the less power scammers have – which is why it's important for us to share our experiences.

It's perfectly normal to feel worried about scams. If reading through this guide makes you feel nervous about getting scammed, there's lots of support available to make sure you can go about your day-to-day life without feeling too worried.

See pages 36-41 for a list of organisations that can provide trusted information and advice.

"I was scammed last year and it really affected my self-confidence. But I spoke to a friend about it and found out he'd had a similar thing. I felt better knowing it wasn't just me."

Alan, 66

Types of scam

This guide covers some of the most common types of scam, ways to spot them and what to do next.

Doorstep scams

Scammers may knock on your door pretending to be people they're not in order to get money out of you.

Find out more on page 10.

Mail scams

You may receive post containing false claims or offers that try to steal your money.

Find out more on page 14.

Phone scams

Scammers could ring up and try to get your personal information or persuade you to buy products you don't need.

Find out more on page 16.

Email and online scams

You may receive emails or come across fake websites pretending to be legitimate or trying to tempt you with fraudulent offers.

Find out more on page 21.

Relationship scams

Some scammers try to earn your trust by forming a pretend relationship in order to get money from you.

Find out more on page 24.

Identity theft

Scammers may try to get hold of your personal details and use them to access your savings or run up debts in your name.

Find out more on page 26.

Investment and pension scams

Scammers may try to steal your pension, perhaps by offering seemingly attractive but fraudulent investment opportunities.

Find out more on page 29.

Doorstep scams

Doorstep scammers often target older people, so it's a good idea to know what to look out for. A scammer may knock on your door and pretend to be a trader, charity collector or simply in need of help. They may seem polite and friendly – but that doesn't mean you can trust them.

Things to watch out for

- Traders who say they've noticed something wrong with your property that they can fix.
- People who come to your door claiming to be police officers or bank staff and ask to see your PIN or your bank cards – the real police and bank staff would never come to your house and ask for this information.
- Pushy sellers who say they have large discounts, time-limited offers or only a few items left.
- People who claim to be from gas and electricity companies but don't have an official ID badge.
- Deliveries of any goods or products that you didn't order.
- 'Charity collectors' who seem pushy or can't supply a registered charity number (you can check details with the Charity Commission – see page 37).
- People who ask to come into your home because they say they need help, for example to use your phone, or because they feel unwell or want to use the toilet.

What to do

You don't have to open the door to anyone you don't know. If you do, always think: **Stop, Lock, Chain and Check**.

- **Stop**: Are you expecting anyone?
- **Lock**: If not, lock any other outer doors before answering the front door, as some scammers may work together.
- **Chain**: Put the door chain on (but remember to take it off again if people with a key, like a carer or cleaner, need to be able to get in). Look through the window or peep hole to see who's there.
- **Check**: Ask for an identity card and examine it carefully. If you're still unsure, phone the company the person says they're from. Get the number from a bill or your phone book. Don't worry about leaving someone waiting – if they're who they say they are, they won't mind. If you're being pressured or feel unsafe, contact friends, family or the police.

Good to know

Do you get uninvited post advertising products and services, for example, pizza delivery flyers or leaflets advertising local businesses? This is junk mail, and while these can be irritating, they aren't always scams. For more information see page 14.

More top tips to avoid doorstep scams

- Never buy from doorstep sellers.
- Ask for a 'No cold callers' sign from your local council or get a printable version online and put it on the front door or in the window.
- Set up a password with your utility providers to be used by anyone they send round so you can be sure they're genuine.
- Don't be embarrassed to say 'No' or ask people to leave.
- Never sign anything on the spot – take the time to think about any offer, even if it seems genuine. Where home improvements are concerned, it's always best to get several written quotes before deciding.
- Don't accept deliveries of anything you didn't order that's addressed to you. If you accept them without realising, contact the company they were sent from or the local police.
- Never hand over your bank cards, cash, jewellery or any other valuable items to anyone claiming to be from the police or from your bank.
- **If it sounds too good to be true, it probably is.**

Good to know

For ways to check someone's credentials, see page 31.
To report a scam, see page 33.

Who to contact

- If you've been scammed on your doorstep, ring Citizens Advice (page 38) and let them know. They'll then pass your report onto Trading Standards.
- If you suspect you've been scammed, contact Action Fraud (page 37).
- To check if someone is genuinely from your phone, energy or water supplier, call up using the number on your latest bill.

To check if a charity is officially registered, contact the Charity Commission (page 37). In Northern Ireland, contact the Charity Commission Northern Ireland (page 37).

- Dial **999** in an emergency or **101** if you're not in immediate danger and want to report the incident.

"After I lost £400 to a doorstep scam, my local Age UK came and placed 'No cold callers' stickers on my door and window. I haven't been bothered since."

Jan, 80

Next steps

See our guide **Staying safe** for more information about rogue traders and staying safe at home.

Mail scams

Mail scams are sent by post and may be addressed to you directly by name. They contain fake claims or offers that are designed to con you out of your money. It's not always easy to control what people send you, but you can control your response.

What to watch out for

- Lotteries or prize draws claiming you've won a fortune. These often look legitimate, with barcodes or ID numbers. The letter will ask you to pay an administration fee, buy a product or call a premium-rate phone number to claim your winnings.
- Bills from companies you don't use. If you receive a bill from a provider and you're not sure if you have an account with them, find the company's contact details in the phone book or online and ask them. Don't use any contact information that's listed on the bill, as it'll likely be set up by the scammer.
- Psychics and clairvoyants who claim to have seen something in your future.
- 'Pyramid' investment schemes, which ask you to pay a fee and recruit friends or family to get a return on your investment.
- People asking for money because of unfortunate circumstances, like illness or poverty.
- Letters from a solicitor about an unclaimed inheritance, often from a relative overseas that you've never heard of.

What to do

- **Reject:** If you receive a letter you think is a scam, ignore it and throw it away. Never reply.
- **Report:** Join the Scam Marshal scheme. You send them your scam mail so they can catch criminals. You can find out more on the Friends Against Scams website (page 39).
- **Ignore:** Don't call any premium-rate phone lines. These numbers start with 09 and calls can cost up to £4 per minute.
- **Verify:** If you're unsure, check the details of the organisation or solicitor.
- **Opt out:** Try to avoid being added to mailing lists. For example, when you register to vote, tick the box to opt out of the 'edited register' (also known as the 'open register'), as this can be used to send unsolicited marketing mail.
- **Reduce:** Register with the Mailing Preference Service (page 39). This will stop many direct-mailing companies from contacting you, but not all of them.

Who to contact

- Tell Royal Mail if you think you've received scam mail and send it to them with a covering letter (page 40).
- Report details of overseas scams to the Citizens Advice consumer service (page 38).
- Contact the Solicitors Regulation Authority (page 40) if you get a letter from a solicitor and aren't sure it's genuine. They can tell you if the solicitor's firm is registered and check a list of reported scams on their website.

In Northern Ireland, contact the Law Society of Northern Ireland (page 39).

Phone scams

Scammers often try to trick people over the phone, so be wary of uninvited or unexpected calls and remember you can always hang up the phone if someone's making you feel uncomfortable.

What to watch out for

- Calls supposedly from your bank or the police about fraudulent use of your bank cards or bank account. Scammers might ask for your PIN and tell you to give your bank card to a courier. Neither your bank nor the police would ever do this.
- Calls from someone claiming to be 'undercover police' saying that they're investigating a member of staff at your bank and asking for your card details. The police would never ask you to help in an investigation like this.
- Pushy sales calls or investment opportunities that seem too good to be true.
- Calls about your computer or mobile phone. The person calling may say your device has a virus and ask you to download software to fix it. This is actually spyware – an unwanted program that runs on your computer and can give scammers access to all your online information.
- Be wary of any cold calls or texts from strange numbers offering products or services, such as pension or debt management.
- Calls claiming to be about correcting your Council Tax band or giving you a Council Tax rebate. Your council would never call you about a rebate out of the blue.

- Calls asking you to pay to renew your membership of the Telephone Preference Service (TPS) (page 41). The service is free and calls asking you to pay for it are scams.
- Calls that seem to be genuine because the caller has information about you. Just because someone knows your basic details doesn't mean they're legitimate. These details can include your name, address, your mother's maiden name and even your Direct Debits.
- Texts asking you to follow a link to fix a problem with one of your accounts or to track a parcel. These links will often take you to fake websites and get you to log in, which scammers can then use to access your information.

"I installed a call-blocking system which has almost stopped all nuisance calls."

Bob, 78

Good to know

A 'cold call' is a phone call out of the blue from a company or person you've never dealt with before, usually trying to sell you something. They aren't always scams, but they can be irritating.

What to do

- **Say no**. Ignore a caller that asks you for personal information such as your PIN or tells you that your computer has a virus. A genuine organisation will never ask you for these details over the phone, in an email or in writing.
- **Report any scams**. Forward unwanted texts to **7726** for free so your mobile phone provider can flag potential scams.
- **Check the line.** Be aware that scammers can keep your phone line open even after you've hung up. Use a different phone, call someone you know first to check the line is free, or wait at least 10 to 15 minutes between calls to make sure that any scammers have hung up.
- **Use an answerphone**. You can use an answerphone on your landline or voicemail on your mobile to screen your calls.
- **Check your calls**. Get a caller ID device to see who's calling. But be aware that some scammers appear as a legitimate number, for example, your bank or utility company.
- **Try call blocking**. Some phones have call-blocking features to stop unwanted calls. If yours doesn't, you can use a separate call blocker. Some blockers come pre-programmed with known nuisance numbers and some allow you to add numbers to that list when you get a nuisance or scam call. You can buy call blockers from various retailers and some local authorities provide them.

- **Cut the cold calls**. Join the free Telephone Preference Service (TPS) (page 41). This should cut the number of cold calls you receive, though it won't necessarily block all scammers. TPS has a service to stop cold calls to mobile phones too. Go to their website or text 'TPS' and your email address to **85095** to register.
- **Call the company.** If you get a phone call from an organisation asking you for personal information, contact the company directly using a known email or phone number to check the call is legitimate.
- **Avoid links.** If you've received a text asking you to follow a link, don't click on it. If you'd like to check if the text is genuine, contact the company directly either using their official website or phone number and enquire about your account that way.

Who to contact

- Contact Action Fraud to report a scam (page 37).
- Contact your bank if you receive a call about your bank account or credit card that concerns you. You can call the centralised number **159** to be connected to them, or call the phone number on the back of your bank card.
- Call, text or go online to TPS to register with its service (page 41). There's a free call blocker to stop scam and nuisance calls available to those identified as most vulnerable by a doctor, Trading Standards officials or local councils.
- Report a scam WhatsApp user by opening the chat with the user you want to report, tapping on their name and then tapping 'report contact'.

Next steps

Ask your landline provider about what call-blocking services they provide – these are normally free to customers.

Email and online scams

Things like email and online shopping can make our lives a lot easier, but they also create opportunities for criminals. Digital scams are becoming increasingly common and sophisticated, so it's good to know how to keep yourself safe.

What to watch out for

- Keep an eye out for fake websites. These often look like a trusted organisation's real website to get you to give personal information. For example, you could get an email claiming to be from your bank, which directs you to a fake website and asks you to enter your account details. A genuine organisation will never contact you out of the blue to ask you for your PIN or full password.
- Any emails from abroad asking for money. It may appear to be a stranded friend or relative asking for help, but is actually a scammer who has broken into ('hacked') that email address. Or it could be an email asking you to transfer a sum of money abroad in return for a larger reward later.
- Emails with attachments, as some attachments contain viruses that infect your computer. These could be from someone you know, but their account may have been hacked.
- Fake tax refund emails which claim to be from HM Revenue and Customs (HMRC) offering you a tax refund if you enter your details. The real HMRC would never email to give you a tax refund. This is a common scam and many people have had money stolen.
- Fake invoice emails that appear to be from companies you deal with regularly, or even a solicitor, and can seem genuine.

What to do

- **Strong password:** Always create a strong password for any online accounts, as this will help prevent your account being hacked. Your email account is a gateway to lots of other accounts, so always use a password you don't use for anything else.
- **Ignore attachments:** Don't open any attachments to an email unless you know they're safe.
- **Leave the links:** Don't click on any links within emails that claim to direct you to your bank, utility company or HMRC. Instead, always search for the website yourself.
- **Check the web address:** Secure websites should always start with **https://** – the 's' stands for 'secure'. You should also look out for a padlock symbol next to the web address – but don't trust a padlock on the actual webpage.
- **Report and delete:** Report scam emails to the government's Suspicious Email Reporting Service at **report@phishing.gov.uk** and then make sure you delete the scam email.
- **Don't reply:** Never reply to scam emails, even to say 'No'. This will let the scammer know that your email address is active and they'll send you more emails.
- **Double-check:** If you get an unexpected request for payment from someone claiming to be a trusted organisation, look up their official phone number and give them a call to check.
- **Filter junk:** Check your email account is set up to filter junk (or spam) mail. This may help remove some suspicious emails from your inbox automatically.
- **Stay virus-free:** Make sure you have anti-virus software installed on your computer to protect it from viruses. Also take the time to install the built-in security measures that most internet browsers offer.

- **Check your preferences:** When shopping online, you may be asked if you want to receive emails from the company. Make sure you tick or untick the correct box. You can also unsubscribe from any mailing list you've joined.
- **Trust your instincts:** If an online offer looks too good to be true then it probably is. Be suspicious of prices that are unusually low.
- **Do your research:** Only use retailers you trust, for example, ones that have been recommended to you. If you're buying an item made by a major brand, you can often find a list of authorised sellers on its official website.
- **Use secure payment methods:** Always use the secure payment methods recommended by trusted online retailers.

Who to contact

- If criminals have gained access to your accounts through an email scam, report it to Action Fraud (see page 37).
- Visit **www.getsafeonline.org** for more advice on how to deal with scam emails, or look at the 'Help' pages of your email account provider.

Good to know

To make a strong password, try using three random words with a combination of capital letters and numbers. Don't use any words or numbers that include personal information, such as your name, street name, house number or date of birth.

The National Cyber Security Centre provides information on how to stay safe online (page 40).

Relationship scams

Dating websites and apps can be a great way to meet someone from the comfort of your own home. But always be careful. Some scammers use these platforms to win people's trust and take their money.

What to watch out for

- Someone asking for personal information, like your full name, address, date of birth or bank details.
- Conversations that get personal very quickly.
- Someone who only tells you vague details about themselves, and nothing that can be fact-checked.
- Someone who quickly suggests talking by email, text or phone rather than via the platform where you met them.
- Emotional stories in which someone asks for money, for example claiming that they've fallen on hard times or that their relative is ill.
- Someone asking you to keep the relationship secret or trying to isolate you from your friends or family.
- Someone asking for money in order to come and visit you because they live far away.

What to do

- **Report and block:** If you become suspicious, most dating platforms and social media sites will let you report a member. You should also be able to block any members that make you feel uneasy or unsafe.
- **Keep safe:** If you arrange to meet someone, meet them in a public place and always let someone know where you'll be.
- **Keep details private:** Don't share too many personal details, such as your full name, date of birth or bank details.
- **Money matters:** Don't send money to someone you've never met in person, no matter what reason they give or how long you've been speaking to them.
- **Check them out:** Have a good look at the person's profile and check they're genuine by putting their name, profile pictures or any repeatedly used phrases and the term 'dating scam' into your search engine.

Who to contact

- If you've lost money in a relationship scam or you think you've been targeted, report it to Action Fraud (page 37).

"I found out Mum had sent over £1,000 to someone she'd met on Facebook."

Amy, 64

Identity theft

Identity theft is when your personal information (like your name, date of birth or address) is stolen and used to commit acts of fraud. These could be things like raiding your bank account, buying goods in your name, or taking out loans or credit cards in your name.

What to watch out for

- Any unfamiliar activity in your bank accounts or missing money that you can't remember spending.
- Post arriving at your house for someone you don't know.
- Changes to your credit rating. For example, if you're refused a loan because your credit rating has worsened unexpectedly.
- You're told you're already claiming government benefits when you apply for them.
- You find out that a mobile phone contract has been set up in your name without your knowledge.

Good to know

You can add two-factor authentication to help secure your accounts. This adds an extra layer of security – it requires another log-in credential and, usually, requires access to a device you own, such as your mobile phone. For example, a unique code might be sent to your phone that you need to log in to your account.

What to do

- **Act quickly:** Cancel any lost or stolen bank cards straight away. If your passport, driving licence, or other personal information has been lost or stolen, contact the organisation that issued it immediately.
- **Double-check:** If you're waiting for a new card or PIN or a new identity document such as a passport, and it's not delivered, alert the organisation responsible straight away.
- **Watch your account:** Contact your bank immediately if there are any transactions on your account you don't recognise.
- **Keep PINs and passwords safe:** Don't write them down or tell them to anyone.
- **Use strong passwords:** Try not to use the same password for more than one account and avoid using obvious passwords or any personal information.
- **Watch your cards:** Always shield your PIN and never let your cards or card details out of your sight when using them to buy something or withdraw money.
- **Stay safe online:** Make sure your computer has up-to-date security software.
- **Phone security:** Lock your mobile phone with a PIN or password. If your phone is stolen, this will stop anyone getting the information on there.
- **Bin carefully:** Shred documents like bank statements and receipts before you throw them away.
- **When you move:** Give your new address to your bank and other relevant organisations and ask Royal Mail (page 40) to redirect your post.

Who to contact

- Visit the identity theft section of the Action Fraud website or call Action Fraud (page 37) for further information on how to prevent identity theft.
- Contact the Citizens Advice consumer service (page 38) for further advice.
- If your details have been stolen before, you might want to register with fraud prevention organisation CIFAS (page 37). For a small fee, it will alert its members to carry out further checks if someone applies for credit in your name.
- Sometimes fraud can be committed using the identity of people who have died. You can contact The Bereavement Register (page 41) to remove the deceased person's details from mailing lists, and the Government's Tell Us Once service (page 39) to inform all government departments of a person's death with just one call.

"I received a parcel for someone I'd never heard of. The whole thing seemed a bit dodgy so I spoke to the local police who said I'd had my identity stolen!"

Jeff, 65

Investment and pension scams

There are many ways that scammers persuade people to part with their pension – from promising investment opportunities that are simply too good to be true, to giving false information. They may call several times and could even have details of any previous investments you've made.

What to watch out for

- Any cold calls about your pension.
- Companies that offer a 'loan', 'savings advance' or 'cashback' from your pension or talk about new investment techniques.
- Offers of investments in stocks and shares in wine, jewellery, carbon credits or land, with rates of return that seem too good to be true, or pressure you to act quickly.
- Offers of 'pension reviews' or new ways to get hold of your pension income before the age of 55 in exchange for a fee, for example by transferring your savings to a different scheme.
- Legitimate products that seem overvalued – for example, shares that exist but have little or no resale value.
- 'Pyramid' investment schemes, where you pay a fee to join and then need to recruit friends or relatives to get a return.
- Offers about investments in cryptocurrency or foreign exchange trading. Most cryptocurrencies aren't regulated by the Financial Conduct Authority, so they're not protected by the UK's Financial Services Compensation Scheme.

What to do

- **Stay calm:** If you get calls offering you investments or access to your pension, don't feel rushed or pressured to respond.
- **Don't commit:** Always seek advice before making decisions.
- **Stop the call:** If you feel pressured or if the caller won't take no for an answer, end the conversation. Don't be embarrassed to put the phone down.
- **Think about foreign fraud:** Be wary of dealing with companies based overseas. They could be located there to avoid important regulatory requirements.
- **Check adverts carefully:** Don't buy from newspaper adverts or marketing leaflets unless you're sure they're genuine. Celebrity endorsements can't always be trusted, as they can be easily faked.
- **Listen to your doubts:** If you think the offer sounds too good to be true, it probably is.

Who to contact

- Check whether companies are authorised by the Financial Conduct Authority (page 38).
- Check the scams warning list at **www.fca.org.uk/scamsmart**.
- Get independent pension advice. Contact the Pension Wise service through MoneyHelper (page 40).
- You could also get advice from an independent financial adviser. You can find a list of registered advisers through MoneyHelper (page 40) or the Personal Finance Society (page 40).
- You can report online scam ads on the Advertising Standards Authority's website (page 37).

Avoiding and dealing with scams

A tradesperson, company, catalogue or website may look professional and sound sincere – but how can you be sure they're legitimate? Here are some ways to check their credentials, and make sure you're not being scammed.

Check their contact details

- Ask for a landline number and phone it to see who answers.
- Be wary if the person only has a mobile phone number and a PO Box address – these are easy to close and hard to trace.
- Visit **www.gov.uk/get-information-about-a-company** to find out a company's details, including its registered address.

If the address is overseas the usual consumer rights may not apply or could be tough to enforce.

Good to know

If in doubt, always get further advice from the Citizens Advice consumer service (page 38).

Check if tradespeople are registered and regulated

- There are various official registration schemes for tradespeople, like the National House Building Council for builders, and Gas Safe for gas engineers.
- Financial services or companies should be regulated by the Financial Conduct Authority (FCA) (page 38).
- If someone claims to be registered, check with the relevant trade organisation or the FCA if it's a financial company.

Check reviews and recommendations

It's always best to get a reliable recommendation if you're buying a product or service. Search online for the company's name to see if there are any reviews. If it's a local business, ask people you know in the area.

It's easy to make convincing business cards and websites, so they don't necessarily prove a person or company's legitimacy.

Still not sure?

- Contact the Citizens Advice consumer service (page 38).
- Contact TrustMark (page 41) to find local tradespeople who comply with government-endorsed standards, or ask your local Age UK for an approved list of traders in the area. In Wales, speak to your local Age Cymru.

Next steps

For more information about different types of scams and what to look out for, download **The Little Book of Big Scams** from the Metropolitan Police website (page 39) or email **cyberprotect@met.police.uk** for a copy.

Reporting a scam

If you've been scammed, it's important to report it right away. You shouldn't feel embarrassed about being scammed – if someone stole your money in the street you'd report it to the police. It shouldn't be any different if a criminal gets access to your private accounts and steals your money. But where should you report a scam?

- **If it's an emergency.** Always call **999** if you or someone else is in danger. You can also call **101** to speak to the police in a non-emergency.
- **If you've had money stolen.** Contact your bank straight away by calling either the centralised number **159** or the phone number on the back of your bank card. They can cancel any cards and freeze your accounts.
- **If you want to report a scam.** Report it to Action Fraud (page 37) to get a crime reference number.

Action Fraud is the UK's national reporting centre for fraud and cybercrime. If you've experienced fraud of any kind, you can report it to Action Fraud over the phone or through their online reporting service. Once you've reported the crime, Action Fraud will pass the case onto the National Fraud Intelligence Bureau to investigate and give you a crime reference number.

Good to know

If you think you've spotted a scam or you'd like some information on different scams, you can call the Citizens Advice consumer service for advice (page 38).

The best thing you can do to protect others from scams and fraud is talk about it. Scams are constantly changing and becoming more sophisticated. By letting relevant organisations know you've been scammed, and telling them how it happened, you can help them keep up to date with the latest scams and help protect others. Not reporting it or not letting others know only helps the criminal scam others.

By reporting it, you might even be able to get some money back. Although this can't be guaranteed, it may be possible in certain circumstances:

- If you paid for something by credit card in a transaction that turns out to be fraudulent, your card provider may offer protection.
- If you have household insurance, your policy may also provide cover in some circumstances.
- If the scammer is traced, it may be possible to prosecute them and recover your money.

Good to know

After reporting a scam, such as a suspicious text message, you may not hear anything back and you won't find out if the scammer's been caught. But reporting scams is worthwhile and does make a difference. More people reporting scams makes it easier to stop the criminals and prevent others from being scammed in the future. Your experience can help keep other people safe from fraud.

Top tips

Here's a handy summary of ways to help you avoid scams.

Don't open emails or attachments from **someone you don't know.**

Your bank will never call you and **ask for your PIN** or for you to give your card to a courier.

With doorstep callers remember: **Stop, Lock, Chain, Check**.

Avoid pension scams by getting **independent advice** before making decisions.

Don't believe letters claiming you have won a fortune. **If you haven't entered** a lottery or prize draw, **you can't have won it**.

Don't be embarrassed to hang up, say no, or ask someone to leave.

Who to contact for further help:
Action Fraud, to report a scam – **0300 123 2040**
Citizens Advice consumer service – **03454 04 05 06**
Victim Support – **08 08 16 89 111**

Useful organisations

Age UK

We provide information and advice for people in later life through our Age UK Advice Line, publications and website.

Age UK Advice: 0800 169 65 65
Lines are open seven days a week from 8am to 7pm.
www.ageuk.org.uk

In Wales, contact Age Cymru Advice: **0300 303 44 98**
www.agecymru.org.uk

In Northern Ireland, contact Age NI: **0808 808 7575**
www.ageni.org

In Scotland, contact Age Scotland: **0800 124 4222**
www.agescotland.org.uk

Action Fraud

Centre for reporting fraud and internet crime in England, Wales and Northern Ireland. Call the helpline for advice on preventing fraud and what to do if you've been scammed or defrauded, or use the online fraud reporting service.
Tel: **0300 123 2040**
www.actionfraud.police.uk

Advertising Standards Authority (ASA)

Independent regulator of advertising across all media in the UK. Use their website to report an online scam advert.
www.asa.org.uk/make-a-complaint/report-an-online-scam-ad.html

The Charity Commission for England and Wales

Regulator for all registered charities in England and Wales. Search on their website for registered charities.
Tel: **0300 066 9197**
www.gov.uk/charity-commission

In Northern Ireland, contact the **Charity Commission for Northern Ireland**
Tel: **028 3832 0220**
www.charitycommissionni.org.uk

CIFAS

Provides a registration service to protect people whose details have been stolen or are considered vulnerable.
www.cifas.org.uk

Citizens Advice

National network of advice centres offering free, confidential and independent advice, face-to-face or by telephone. Visit their website for online information and to find details of your nearest Citizens Advice.
In England, call Adviceline: **0800 144 8848**
www.citizensadvice.org.uk

In Wales, call Advicelink: **0800 702 2020**
www.citizensadvice.org.uk/wales

In Northern Ireland: **www.citizensadvice.org.uk/about-us/northern-ireland**

Citizens Advice Consumer Service

Provides information and advice on consumer issues by telephone and online. Offers tips on avoiding scams.
Tel: **0808 223 1133**
Welsh-speaking adviser: **0808 223 1144**

Financial Conduct Authority (FCA)

Provides advice on choosing a financial adviser. The FCA has a scam warning tool on their website for checking if an investment offer might be a fraud and online register you can use to check whether a company is authorised by the FCA.
Tel: **0800 111 6768**
www.fca.org.uk
ScamSmart Investment checker: **www.fca.org.uk/scamsmart**
Financial services register: **register.fca.org.uk/s/**

Financial Ombudsman Service

You can escalate complaints using this service if you're not satisfied with how your bank or building society has treated you after you've reported a scam.
Tel: **0800 023 4567**
www.financial-ombudsman.org.uk

Friends Against Scams
Offers information as well as schemes such as the Scam Marshals scheme.
www.friendsagainstscams.org.uk

Get Safe Online
Government-backed website that gives free advice and tips on using the internet securely.
www.getsafeonline.org

GOV.UK
Government website of services and information, with advice on crime prevention and the Tell Us Once service.
www.gov.uk
www.gov.uk/find-local-trading-standards-office

Law Society of Northern Ireland
Can check if a solicitor is registered in Northern Ireland.
Tel: **028 9023 1614**
www.lawsoc-ni.org

Mailing Preference Service (MPS)
Free register for individuals who don't want to receive unsolicited sales and marketing contacts by post.
Tel: **0207 291 3310**
www.mpsonline.org.uk

Metropolitan Police
Contact them in non-emergency situations to access their specialist scams publications and advice.
Tel: **101 (non-emergency)**
www.met.police.uk

MoneyHelper

Gives impartial information about financial products and services and offers tips on everyday money management. Its Pension Wise service offers guidance about your pension, as well as free appointments with an adviser.
Pensions Helpline: **0800 011 3797**
Money Adviceline: **0800 138 7777**
www.moneyhelper.org.uk

National Cyber Security Centre

Provides information and advice about staying safe online.
www.ncsc.gov.uk

Personal Finance Society

Can help you understand what financial choices you have and allows you to search for a qualified financial adviser.
Tel: **020 8530 0852**
www.thepfs.org

Royal Mail

If you or someone you know is receiving scam mail in the post, you can report it to the Royal Mail. You can post your letter directly to FREEPOST SCAM MAIL.
Tel: **0800 011 3466**
Email: **scam.mail@royalmail.com**
www.royalmail.com

Solicitors Regulation Authority

Regulates solicitors and law firms across England and Wales. You can check if a law firm or individual solicitor is registered with them, and their website has a scam alert section.
Tel: **0370 606 2555**
www.sra.org.uk

Telephone Preference Service (TPS)
Free opt-out service for individuals who don't want to receive unsolicited sales and marketing telephone calls.
Tel: **0345 070 0707**
www.tpsonline.org.uk

The Bereavement Register
Register the name and address of a deceased person to help stop unsolicited mail.
Tel: **020 7089 6403**
www.thebereavementregister.org.uk

Think Jessica
Campaign against scam mail. Includes stories of scam mail victims, along with resources for help and advice.
Email: **advice@thinkjessica.com**
www.thinkjessica.com

TrustMark
Organisation that helps you to find a reliable, trustworthy tradesperson.
Tel: **0333 555 1234**
www.trustmark.org.uk

Unbiased
List of qualified, independent financial advisers in your area.
Tel: **0800 023 6868**
www.unbiased.co.uk

Victim Support
Charity that provides free and confidential help to victims and witnesses of crime in England and Wales.
Tel: **08 08 16 89 111**
www.victimsupport.org.uk

In Northern Ireland, contact **Victim Support NI**
Tel: **02890 243133**
www.victimsupportni.com

Can you help Age UK?

If you're able to, please complete the donation form below to make your gift and return to: **Freepost Age UK REPLY**. Alternatively, you can phone **0800 077 8751** or visit **www.ageuk.org.uk/donate**. If you prefer, you can donate directly to one of our national or local partners. Thank you.

Your details

AGUK0081 MXAQ23CA04C015

Title: Forename: Surname:

Home address:

Postcode:

Email address:

We'd† like to keep in touch with you to tell you about the vital work we do for older people, our fundraising appeals and opportunities to support us, as well as the products and services you can buy.

Please tick the boxes to let us know how you'd like to hear from us:

☐ **I would** like to receive communications by email.

We will never sell your data and we promise to keep your details safe and secure.

☐ **I do not** wish to receive communications by post.

If you don't want to hear from us, or change your mind about how we contact you, please email **contact@ageuk.org.uk** or call **0800 169 8787**. For further details on how your data is used and stored by the Age UK network go to **www.ageuk.org.uk/help/privacy-policy.**

Your gift

Please accept my one-off gift of: **£10** ☐ **£15** ☐ **£20** ☐ **My choice £**

☐ I enclose a cheque/postal order made payable to Age UK, **or**

I wish to make payment by (please tick):

☐ MasterCard ☐ Visa ☐ CAF CharityCard

Card number Expiry date

Age UK provides a range of services and your gift will go wherever the need is the greatest.

Help us be there for someone else

We hope you found this guide helpful. When times are tough, it's so important to get some support. Did you know you could help us reach someone else who needs a little help? Here's how:

Give your views on guides like this

Our Readers' Panel helps make sure the information we produce is right for older people and their families. We'd love you to join. Go to **www.ageuk.org.uk/readers-panel**.

Donate to us

Every donation we receive helps us be there for someone when they need us. To make a donation, call us on **0800 169 8787** or go to **www.ageuk.org/donate**.

Volunteer with us

Our volunteers make an incredible difference to people's lives. Get involved by contacting your local Age UK or at **www.ageuk.org.uk/volunteer**.

Campaign with us

We campaign to make life better for older people, and rely on the help of our strong network of campaigners. Add your voice to our latest campaigns at **www.ageuk.org.uk/campaigns**.

Remember us in your will

A gift to Age UK in your will is a very special way of helping older people get expert support in the years to come. Find out more by calling **020 3033 1421** or visit **www.ageuk.org.uk/legacy**.

What should I do now?

You may want to read some of our relevant information guides and factsheets, such as:

- **Looking after your money**
- **Staying safe**
- **Advice for carers**

You can order any of our guides or factsheets by giving our Advice Line a ring for free on **0800 169 65 65** (8am-7pm, 365 days a year).

Our friendly advisers are there to help answer any questions.

All of our publications are available in large print and audio formats.

There's plenty of really useful information on our website, too. Visit **www.ageuk.org.uk/scams** to get started.

If contact details for your local Age UK are not in the below box, call Age UK Advice free on **0800 169 65 65.**

0800 169 65 65
www.ageuk.org.uk

ID204992 07/23