

Protect yourself from scams

How to recognise, avoid and safely deal with scams



A guide by

JEWISH CARE



Contents

What this guide is about	4
What is a scam?	4
Rebecca's story: A real-life example	5
What are the different types of scams?	7
Online and email	8
Doorstep	10
Phone and text	12
Postal	14
Relationship	16
Identity theft	18
Pension and investment	20
Useful organisations and resources	22

**If you have been the victim of a scam,
you are not alone.**

If you don't know where to turn, our Jewish Care Direct helpline can help. Our advisors will listen, give you the information you need, and find the right services to support you.

Call **020 8922 2222**, email helpline@jcare.org
or visit www.jewishcare.org

What this guide is about

We all want to keep our money safe and protected from criminals. Falling victim to a scam puts your money at risk, having a big impact on your finances, your emotions and how safe you feel.

As technology has progressed, scams have become increasingly sophisticated and difficult to avoid. They come in many different forms, making it difficult to know how to protect yourself in all areas.

This guide provides an overview of how to avoid falling victim to a scam, breaking it down into simple steps. It also explains what you can do if you are targeted by a scam. Following this guide can help to keep yourself, your personal information, and your money safer.

This guide answers the following questions:

What is a scam?

What are the different types of scams?

How can I spot and avoid scams?

What should I do if I am targeted by a scam?

Where can I get further information, advice and support about scams?

What is a scam?

A scam is a fraudulent scheme that is designed to get hold of your money.

The person who carries out the scam is called a scammer.

A scammer can seem friendly and pleasant but uses dishonest means to steal your money. They can be very realistic; victims believe they are dealing with a genuine person or organisation.

Scams vary in size and complexity. They can be very quick or last for years. The amount of money they take can range from a few pounds to entire life savings.



Rebecca's story: A real-life example

"One day my mum's carer called me sounding alarmed. She had entered mum's house and discovered a man sitting on the sofa smoking a cigarette.

He was supposedly a charity collector who had asked to use her toilet, so she let him in. Thankfully, he left on the carer's request. When I spoke to mum, she felt it would have been rude not to let him in. We were shaken up, but she seemed unharmed.

Mum suffered a stroke shortly after and went to hospital. I checked on the house and discovered that all her jewellery was missing. The man must have lied to earn her trust, gain entry to the house, then steal her jewellery when he 'used the toilet'.

I reported it to the police but there was nothing they could do. Mum had willingly let him in. For all we know she could have given her jewellery away. Because of mum's stroke, she was unable to confirm if this was true or not.

Mum died shortly after. It is distressing that she was taken advantage of during the last weeks of her life. We were lucky that no greater harm was done, however it saddens me that none of her jewellery is here to remember her by.


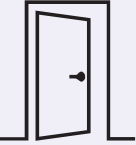



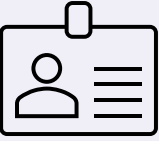

In hindsight, I was so fixed on meeting her care needs that I didn't consider the harm that could be done by scams. My advice would be to educate yourself and the people you support about scams. Mum and I could have talked about how to keep herself safe. It might have stopped this incident from happening."



What are the different types of scams?

There are many different types of scams to avoid. There are also different ways to deal with a scam, depending on which type it is.

Here are the main types to be aware of:

	Online & email Page 7	Fake emails, text messages and websites pretend to be legitimate to get your personal information and money.
	Doorstep Page 9	Scammers can knock on your door to target you in many ways, from asking to come inside, to offering you fake goods and services.
	Phone & text Page 11	Fraudulent phone calls and text messages can get you to hand over your personal information and money.
	Postal Page 13	You can receive mail containing false offers and claims trying and get your money.
	Relationship Page 15	Scammers will form a relationship or friendship with you to earn your trust.
	Identity theft Page 17	Your personal information can be used to make purchases and run up debts in your name.
	Pension & investment Page 19	Scammers can persuade you to transfer your savings or pension into unusual, high risk investments, or outright steal them.

Online and email scams

There are many fake emails and websites that are trying to scam you. They do a good job of tricking people into believing they are real, because they often look legitimate and have a sense of urgency.



Example

You get an email from a delivery company that you know of. It says you need to pay a fee, otherwise your package will not be delivered. You click the link to their website, fill in some personal details and pay the fee. This was a scam – there was no package, the email was fake, the link took you to a fake website and you handed over your money and personal information.

What to look out for

- **Look at the address the email has been sent from.**

A company email that comes from a public domain such as @gmail.com is not legitimate. Even Google uses an official domain (@google.com).

The email address may be misspelled to look close to the official domain (e.g., @gooogle.com – there is an extra 'o').

- **Check the web address of any link before you click on it.**






If it does not look right or match the context of the message (e.g., it is misspelled or it does not look official), do not open it.

To do this using a computer or a laptop, hover the cursor over the link. If this does not work, you should be able to copy the link address and paste it elsewhere so you can inspect it. To do this with a touch screen, press and hold your finger on the link.

- **Poorly written emails and websites.**

Often the grammar is incorrect. There can be spelling mistakes too, however scammers will often use a spell checker.

Top tips for avoiding online and email scams

-  Never open an email attachment (such as an invoice) unless you are fully confident the message is from a legitimate party.
-  Do not click on an email link even if it is from a trusted organisation (such as the bank, HMRC, or utility company). Type in their official web address instead.
-  Use strong and unique passwords for each online account.
-  Make sure your email settings filter out junk mail. This should catch and remove a lot of scam emails from your main inbox.
-  Install anti-virus software on your devices.

What to do if you are targeted by an online or email scam

- **Do not** click on any links, or attachments, or reply to the email.
- **Do not** give any personal or banking information.
- **Do** report it to Action Fraud (www.actionfraud.police.uk), then delete the email and close the website.
- **Do** contact your bank as soon as possible if you have made a payment in response to a scam.

Received an email from Jewish Care?

Emails from Jewish Care always end in **@jcare.org**

You can make sure you are using the real Jewish Care website by typing:
www.jewishcare.org into your web browser.



Doorstep scams

Scammers can turn up at your home to target you in many ways, from asking to come inside to selling you fake goods and services from your doorstep. The face-to-face element can make it more challenging to deal with than other types of scams.







Example

A tradesperson knocks on your door to say they've noticed your guttering needs cleaning – if it's not cleaned soon, you will have a problem on your hands. You are unsure but they are persistent, so you agree to the work. They insist on being paid cash upfront, and you go inside while they work. The work takes a lot quicker than you expected, and after they leave you can't see much difference to the guttering. This was a scam – the 'tradesperson' was not legitimate and did not carry out the work you paid them for.

What to look out for

- **Anyone** you do not know who asks to come in for any reason, such as to use the phone or toilet.
- **Anyone** who keeps you distracted at your front door – they may have an accomplice trying to get into your home through your back door.
- An **unsolicited salesperson** pressuring you into buying something.
- An **unsolicited tradesperson** knocking on your door.
- **They may say** they have noticed work that needs doing on your home that they can fix, and that it is urgent or ask for immediate payment. They might claim they are working next door, so they need to come inside to look at something in your property. Check with your neighbour before letting them in.

Top tips for avoiding doorstep scams

-  Never give money or your banking information to anyone who shows up at your door – even police officers.
-  Put a sign on your door that says 'no cold callers'.
-  Keep your back doors locked when you answer the front door.
-  Only let people into your home who you trust. Make prior arrangements with anyone else. If you need to let someone you do not know inside, do all you can to confirm that they are a legitimate person beforehand.

You can ask to see their ID if they are from an organisation. Check it carefully and call the company to ensure the person works for them. To check if someone is genuinely from your energy, phone, or water supplier, call the number on your latest bill. To check if a charity is officially registered, check via the Charity Commission (www.gov.uk/charity-commission).

What to do if you are targeted by a doorstep scam

In the case of emergency call 999.

- **Do not** give any personal information or money, or let them in.
- **Do** say no and close the door.
- **Do** report the incident to the police by calling 101 (if you are not in immediate danger), and Action Fraud (www.actionfraud.police.uk).
- **Do** contact your bank as soon as possible if you have made a payment in response to a scam.

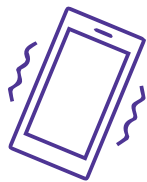
Has someone from Jewish Care knocked on your door?

We **do not** use doorstep charity collectors, however there may be times we do knock on your door. For example, to deliver Meals on Wheels that you have pre-ordered. Jewish Care will never turn up at your door without confirming with you beforehand by phone or email.

If someone at your door claims to be from Jewish Care, you can call us on **020 8922 2222**. They will liaise with colleagues in the relevant department to confirm if a Meals on Wheels delivery is expected, or any other sort of visit.

Phone and text scams

Fraudulent phone calls and text messages are very common. The content of these can range from your bank supposedly alerting you to fraudulent activity on your account, to a fake computer company saying there is a virus on your computer and that they help to eliminate. It is important to exercise caution and scepticism about who is calling or texting you.









Example

You receive a phone call from HMRC saying you are due a tax rebate. You are pleasantly surprised by this news. The person says that to proceed, you need to provide some personal and banking information to confirm it is you and so they can process the rebate. After the phone call has ended, you discover that money has been taken from your bank account. This was a scam – this wasn't HMRC and there was no rebate.

What to look out for

- They are pushy, aggressive or rush you into making a decision.
- It is from an unknown number (but not always).
- They ask for an account password or PIN number.
- They are evasive if you have questions. Ask for proof of where the caller is from – they might change the subject or make you feel bad for asking.
- Poorly written text messages. Often the grammar is incorrect. There can be spelling mistakes too, however scammers will often use a spell checker.
- Check the web address of any link before you click on it. To do this with a touch screen, press and hold your finger on the link. If it does not look right or match the context of the message (e.g., it is misspelled or it does not look official), do not open it.

Top tips for avoiding phone and text scams

-  Do not answer calls or engage with texts from an unknown number.
-  Do not click on a link in a text message even if it is from a trusted organisation (such as the bank, HMRC, or utility company). Type in their official web address instead.
-  Use your voicemail or answerphone to screen the call before calling back.
-  Ask to hang up and call back using the company's official phone number. A genuine company will not mind this, but make sure you verify that the phone number you use is real.
-  Check the line is clear before using your landline. Scammers can keep the line open. Wait at least ten minutes after hanging up to use the phone, even if it is to check with the company that the caller is legitimate.
-  Register with the Telephone Preference Service to reduce the amount of marketing and sales calls you receive (www.tpsonline.org.uk).

What to do if you are targeted by a phone or text scam

- **Do not** click on any links or reply to the text.
- **Do not** give any personal or banking information.
- **Do** say no and hang up the phone.
- **Do** forward spam texts to 7726 free of charge to report them.
- **Do** report it to Action Fraud (www.actionfraud.police.uk).
- **Do** contact your bank as soon as possible if you have made a payment in response to a scam.

Has someone from Jewish Care phoned you?

Jewish Care will **never** phone you in an unsolicited way to sell you a product or service, even if it is free of charge.

If Jewish Care phones you, you are welcome to make the recommended checks to confirm it is a legitimate phone call. Ask for the caller's name and department, hang up and call us on **020 8922 2222** (wait at least ten minutes if using a landline), and ask to speak to the person who called. You can also call this number to confirm a text message from Jewish Care is legitimate.

Postal scams



Mail can be fraudulent, even if it is addressed to you. Spotting the difference between junk mail, scam mail and offers from legitimate companies can be difficult.

Example







You receive a letter addressed to you, congratulating you on winning a cash prize from a competition you entered a few months ago. You do not remember the competition, but you are excited to have won. The letter states that to claim your prize you need to call a premium rate number and pay a fee. After doing so, no prize materialises. This was a scam – the letter and competition were fake, the phone call was expensive and there is no prize.

What to look out for

- Pyramid schemes, chain letters and investment opportunities.
- Letters from people you don't know asking for money. Even if they have been through hard times and are asking for your help.
- An unexpected windfall or offer of a reward.
- Prize draws, competitions and lotteries.
- Unclaimed inheritance from a relative you haven't heard of.
- Psychics who 'predict' a future windfall.
- Requests to complete a task in exchange for a reward.



Top tips for avoiding postal scams

-  Do not call any premium rate numbers mentioned within a letter. These often begin with 09 and are expensive.
-  Contact the company to verify the letter is legitimate, if you believe it could be from a trusted organisation. Do this by using their official website address, then use the contact details listed there. Do not use any contact details contained within the letter.
-  Put a sign on your door that says 'no junk mail'.
-  Opt-out of the 'open register' when registering to vote.
-  Ignore and discard any letter you are suspicious of.
-  Register with the Mailing Preference Service to reduce the amount of spam mail sent to your address (www.mpsonline.org.uk).

What to do if you are targeted by a postal scam

- **Do not** respond to the letter in any way.
- **Do not** give any personal information or money.
- **Do** send it to Royal Mail with a covering letter (see page 22 for contact details).
- **Do** contact your bank as soon as possible if you have made a payment in response to a scam.

Have you received mail from Jewish Care?

All official Jewish Care correspondence contains our registered charity number: 802559.

To check with us that the mail you have received is legitimate please call us on **020 8922 2222**.

Relationship scams

Scammers can earn your trust over time by forming a romantic relationship with you, then ask you for money for a variety of emotive reasons which are untrue (such as fake medical or travel costs).



Example

You start a romantic relationship with someone you met on a dating site. They live far away so you have not met, but you do talk a lot over the telephone. They say it is a struggle to talk with you because their phone is broken, so on their request you send them £800 for a new phone. When you decide it is time to meet, they cannot afford the travel costs and ask to borrow £150 from you. They then cancel at the last minute due to an emergency. This was a scam – they entered into the ‘relationship’ with the intention of taking your money, and it will continue until you end all contact with them.

What to look out for

Someone who does any of the following:

- Professes their love or gets personal quickly.
- Claims to need money for an emergency or for the travel costs to see you.
- Asks you to keep the relationship secret from your family and friends.
- Only gives vague information about themselves.
- Asks for your bank details or personal information such as your date of birth and address.

Top tips for avoiding relationship scams

- ✗ Never share unnecessary personal information, such as bank details, your full name, address, or your date of birth.
- ✗ Never send money to someone you have not met.
- ✓ Check the person is genuine. Put their name, pictures, and phrases they use into a search engine, with the words 'dating scam'.
- ✓ If an online love interest asks you for money, walk away.
- ✓ Always meet in a public place and tell someone where you are.

What to do if you are targeted by a relationship scam

- **Do not** continue to respond.
- **Do not** give any personal information or money.
- **Do** block them.
- **Do** report it to Action Fraud (www.actionfraud.police.uk).
- **Do** contact your bank as soon as possible if you have made a payment in response to a scam.



Identity theft

Identity theft occurs when a scammer uses your personal information to make purchases, open bank accounts and run up debts in your name. You may not even realise it has happened.



Example

You check your credit report and discover a payday loan was taken out in your name that you are unaware of, and that you are required to pay back. This was a scam – criminals stole your personal information and used it to get your money.

What to look out for

- Unusual or unfamiliar activity on your bank account.
- A sudden decrease in your credit score, which you cannot account for.
- Packages that arrive to your home addressed to someone you do not know, especially if someone comes by to collect it.

Top tips for avoiding identity theft

- ✗ Do not write down or tell anyone your passwords or PIN numbers.
- ✗ Do not wait too long to receive a new bank card, PIN number, driving licence or passport. Tell the organisation if it has not arrived.
- ✓ Use strong and unique passwords for each account.
- ✓ Always keep sight of your bank cards when using them out and about.
- ✓ Cover your PIN number when you are typing it in to a machine.
- ✓ Cancel lost or stolen bank cards immediately.
- ✓ Make sure your phone is secure by using a password or other method of locking it.
- ✓ Destroy documents with personal and banking information such as receipts and bank statements (i.e., with a shredder).

What to do if you are targeted by identity theft

- **Do** contact your bank as soon as possible if you do not recognise a payment made from your account.
- **Do** report it to Action Fraud (www.actionfraud.police.uk).
- **Do** register with CIFAS who can alert you if a credit application is made in your name for a small fee (www.cifas.org.uk).



Has Jewish Care asked you for personal information?

At Jewish Care we may ask for, hold, and process your personal information when you interact with our various departments and services.

Your privacy is important to us. Our Privacy Notice explains how we keep your information protected and confidential.

Visit www.jewishcare.org/privacy-statement for more information.

Pension and investment scams

Scammers can persuade you to transfer your savings or pension into unusual, high risk investments, or outright steal them from you.



Example





You come across advice promoting an attractive investment opportunity – there is a tip that if you buy shares of a specific up-and-coming wine producer with great prospects this week, you will get a big return on your investment in a short space of time. This seems like an exciting opportunity, so you go for it. True to their word, the price increases rapidly, however it crashes shortly after, and you lose all your money. This was a scam – these were false tips designed to get people to invest and raise the share price. The scammers then sold their share at peak price, causing the price to go down.

What to look out for

- Anything that is too good to be true – it probably is.
- Companies that are based overseas (this means they could be avoiding regulations).
- Companies that rush or pressure you into making a decision.
- Companies that offer the following schemes:
 - Cashback or an advance from your pension.
 - New investment techniques or new ways to access your pension early.
 - Pyramid schemes.



Top tips for avoiding pension and investment scams

-  Do not engage with cold calls about your pension or investment opportunities.
-  Check the company is authorised by the Financial Conduct Authority (www.fca.org.uk). You can also check their scams list.
-  Seek independent pension or financial advice before making a decision.
-  It is okay to decline if you are feeling pressured.

What to do if you are targeted by a pension or investment scam

- **Do not** respond in any way.
- **Do not** give any personal information or money.
- **Do** report it to the Financial Conduct authority (www.fca.org.uk).
- **Do** contact your bank as soon as possible if you have made a payment in response to a scam.

Have you received financial advice or services from someone at Jewish Care?

At Jewish Care we recommend that you seek independent financial advice when considering paying for care, or moving into a care home, or moving to Retirement Living.

No one at Jewish Care will ever offer financial, pension or investment advice in relation to accessing our services.

Useful organisations and resources

Jewish Care Direct helpline

If you have been the victim of a scam and don't know where to turn, we can help. Our advisors will listen, give you the information you need, and find the right services to support you. 020 8922 2222 helpline@jcare.org www.jewishcare.org

Action Fraud

The UK's national reporting centre for fraud and cybercrime.

www.actionfraud.police.uk

Age UK

Help, information, and advice for older people.

www.ageuk.org.uk

Charity Commission

The regulator for charities in England and Wales, where you can check a charity is legitimate.

www.gov.uk/charity-commission

CIFAS

The UK's largest cross-sector fraud sharing organisation. You can join their Protective Registration service to reduce the risk of identity theft.

www.cifas.org.uk

Citizens Advice Consumer Service

Get advice on your consumer rights, including complaints and trading standards.

0808 223 1133

www.citizensadvice.org.uk

Financial Conduct Authority

Regulates the financial services industry in the UK. You can report investment scams to them.

0800 111 6768

www.fca.org.uk

Mailing Preference Service

Removes your name and address from mailing lists, to reduce the likelihood of receiving scam mail.

0845 703 4599

www.mpsonline.org.uk

The Pensions Advisory Service

Free information and advice about your pension. 0800 011 3797

www.gov.uk/pensions-advisory-service

Royal Mail

Forward scam mail to Royal Mail with a cover letter.

Post: Freepost Scam Mail,

PO Box 797, Exeter EX1 9UN

Email: scam.mail@royalmail.com

Phone: 0345 611 3413

Web: www.royalmail.com

Telephone Preference Service

The UK's only official 'Do Not Call' register for landline and mobile numbers. 0345 070 0707

www.tpsonline.org.uk

Trading Standards

Complain about illegal sales activity.

www.gov.uk/find-local-trading-standards-office

UK Government

Get information about to company to help check its legitimacy.

www.gov.uk/get-information-about-a-company



If you have been the victim of a scam, you are not alone.

If you don't know where to turn, our Jewish Care Direct helpline can help. Our advisors will listen, give you the information you need, and find the right services to support you.

**Call 020 8922 2222, email helpline@jcare.org
or visit www.jewishcare.org**

Thank you to Age UK whose resources have helped in creating this guide

JEWISH CARE

Charity Registration Number 802559