



Avoid falling prey to fraudsters

Every year the British public loses billions of pounds to fraudsters who bombard us with online messaging, mail, door-to-door and telephone scams.

People of all ages, backgrounds, and income levels can fall victim to these scams and as time goes on, fraudsters are finding new ways of targeting individuals. This guide will help you to identify the different types of scam and outlines the ways in which you protect your lifetime mortgage by avoiding them.

Identity Fraud



Scammers use an individual's personal details to sell onto others or commit crimes such as opening bank accounts and taking out loans or credit cards.

- Your personal information is valuable: make sure you protect it.
- When disposing of anything showing your personal or banking details, use a shredder or tear it up into small pieces.
- If you start to receive bills, invoices, or receipts for goods you didn't purchase, find out why.
- If you start to receive post for someone you don't know, find out why.

Holiday Fraud



Scammers are targeting online holiday booking, accommodation, and comparison sites to scam unsuspecting customers into paying for accommodation that isn't available or doesn't exist. This can be for both destinations overseas and in the UK. Often the victim only becomes aware when they arrive at their destination.

- Be aware that if it sounds too good to be true, it probably is.
- Check the web address is legitimate and hasn't been altered by a slight change such as **.co.uk** to **.org**
- Only give out personal and financial information to companies that you trust and have given consent to be contacted by.
- Be wary of emails, online advertisements or cold calls asking for bank details in order to refund cancellation fees or offering compensation that you may already have.

Courier Fraud



Scammers will call a potential victim pretending to be from their bank or the police. They then persuade the person to reveal their PIN and hand over their debit or credit card details.

- Your bank or the police will never ask for your PIN, your bank card or to withdraw money.
- The police will never phone you to ask for donations or payments needed to aid in an investigation or to acquire high value items for you.
- Never share your PIN with anyone.
- Never hand your bank card or any goods you've bought following a phone call to anyone who comes to your front door

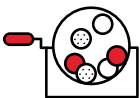
Banking and payment card scams



Card scams involve using stolen or counterfeit cards to make purchases or cash withdrawals.

- Never share your PIN with anyone.
- Check your statements regularly to make sure they're correct.
- Remember, your bank and the police will never ring you and tell you to verify your PIN number, withdraw cash or buy high value goods. They will also never tell you that they're coming to collect these items.

Lottery and prize draw scam mail



Fraudsters lure people with the thrill of a surprise win only to find themselves parting with large amounts of money to claim these fake prizes. There is a huge range and variety of mass market mail, some of which will be obviously fraudulent and others that won't.

- Whatever the case you should be very careful what you reply to and be wary of mail from competitions you haven't entered.
- Genuine lotteries or competitions won't ask you to pay a fee to collect your winnings.
- Never send money abroad or to someone you don't know or trust
- Don't provide banking or personal details to someone you don't know and trust.

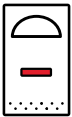
Health Scams



Scammers will contact people via email or text, promising help or offering to arrange official appointments for common health issues.

- Your GP or the NHS will never ring or email you to ask for your PIN number, banking details or to withdraw cash in order to set up an appointment.
- Do not fall for quick fixes, miracle cures or scientific breakthroughs.
- Contact your GP if you are unsure about an appointment you didn't ask for or arrange.
- Don't give out your personal details to someone you don't know or trust.

Doorstep Scams



Scammers may go door to door offering services or work that you do not need such as building works or assistance with finances.

- Don't feel pressurised to hand over money or sign up to services you don't need.
- Only let someone in if you know them or are expecting them. Do not feel like you can't turn them away.
- Never share your bank information with them or hand over your card for them to 'check'.

Romance Scams



Fraudsters may make contact via dating apps, email or social media and go to great lengths in order to build up a "relationship" before asking for financial support in the form of money or expensive gifts. Whilst some relationships can be genuine, you should be very careful when someone starts to ask you for money:

- Check that someone is who they say they are and make sure that their photos are not associated with other names or websites.
- Be wary if they do not wish to meet in person or want to keep it a secret.
- Do not respond to people asking you for bank transfers of large amounts or the purchase of expensive gift cards and electronic devices.
- Do not be afraid to ask friends and family members for advice.

Internet scams



Scammers may use emails or weblinks to attempt to put programmes on your computer that can steal, wipe or lock your data.

- Make sure you have antivirus software and a firewall installed on your computer and keep them up to date.
- Don't click on any links or call any numbers shown in the email if you are suspicious of it.
- Don't reply to spam emails, even to unsubscribe.
- Delete all messages without reading them if they're from someone you don't know or trust.

Investment scams



Victims are contacted by letter, phone or email and told that investing in some type of scheme is a guaranteed way of making money, often offering exclusive opportunities in appealing markets such as cryptocurrencies and agricultural land.

These types of scams are popular because scammers can also easily produce authentic looking emails, websites and paperwork as well as setting up virtual offices.

- Don't respond to callers trying to sell you investments. Simply hang up the telephone or delete the email. Legitimate investment companies will never cold call or send spam emails.
- Don't let the company pressure you into buying because they say the offer won't be there tomorrow.
- Be very careful when investing your money and speak to a financial adviser if you have any questions.

Protecting yourself and others

Remember that if you're a victim of a scam or an attempted scam, however minor, there may be hundreds or thousands of others in a similar position. Your information may form part of one big jigsaw and may be vital to completing the picture.

If you think you've uncovered or been targeted by a scam or fallen victim to one, you can contact Action Fraud Police to make a report.

Call:

0300 123 2040

Visit:

www.actionfraud.police.uk

For more information about how you can protect yourself against scams visit Friends Against Scams:

www.FriendsAgainstScams.org.uk

Friends Against Scams is a National Trading Standards (NTS) Scams Team Initiative, which aims to protect and prevent people from becoming victims of scams.

If you feel that your lifetime mortgage has been affected by or is at risk from a scam, call our Customer Services team:

03330 048444

Lines are open 8.30 am to 5.30pm Monday to Friday.

Call charges will vary. Calls may be monitored and recorded.

Alternatively, you can email us at

customerservices@landghomefinance.com

If you're contacting us by email please remember not to send any personal, financial or banking information because email is not a secure method of communication.

Legal & General Home Finance Limited is a wholly owned subsidiary of Legal & General Group plc. Registered in England and Wales number 04896447.

Registered office: One Coleman Street, London EC2R 5AA.

Legal & General Home Finance Limited is authorised and regulated by the Financial Conduct Authority. Q0056299 LG001509 04/21

