



Are you or your loved ones being targeted by scams?

**Help to manage finances and avoid scams for
people at risk and those who support them**





Contents

3 About this guide

4 Introduction

5 What to do if you think you have responded to a scam

6 **PART ONE: Stopping criminals from reaching you**

Mail Scams

7 Scam calls

8 Doorstep scams

9 Internet scams

10 Other practical advice

11 **PART TWO: Help a friend or relative with their finances**

12 What is a Lasting Power of Attorney (LPA)?

13 Types of Lasting Power of Attorney
Things to consider when appointing an attorney

14 Registering as an attorney with the bank
More help and advice on LPAs and managing your finances

15 Useful signs

About this guide

This guide has been brought to you by the National Trading Standards Scams Team and the National Centre for Post Qualifying Social Work and Professional Practice at Bournemouth University, working in partnership with Lloyds Bank, Halifax and Bank of Scotland. Our teams have been leading research on scams and fraud across the UK. We work closely with people who have fallen victim to scams and we use their insights to help protect others. The advice in this guide is based on our knowledge and practical experience of what works.

Introduction

If you are worried about becoming a victim, or have responded to scams in the past, this guide sets out some practical things you can do to prevent criminals contacting you. It also gives information on how you can nominate a trusted friend or relative to help manage your finances if you need help to make decisions.

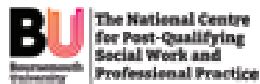
If you are concerned about a friend or relative, you can also use the tips in this guide to help protect them from scams.

Remember that the criminals who set out to trick you into sending them money are extremely clever and sophisticated. They may spend hours researching you or weeks building up a relationship of trust. They will use pressure tactics to make you give them what they want.

Anyone can fall victim to a scam, but some people are more susceptible than others because of their circumstances. People living with some form of cognitive impairment, such as dementia, may be unable to distinguish scams from legitimate opportunities.

The National Trading Standards Scams Team created the Friends Against Scams initiative to protect and prevent people from falling victim to this type of crime.

For further information on how to spot a scam, complete the awareness session to become a Friend Against Scams. Go online to www.friendsagainstscams.org.uk or look out for scams awareness events in your area.



What to do if you think you have responded to a scam

If you do respond to a scam, whether by post, telephone, internet, email or on the doorstep, it's important that you report it quickly so that you get the right support. Don't be embarrassed to talk to friends and family to get their help – remember that you have been the victim of a sophisticated crime.

Remember -
scams are a
crime. Don't be
embarrassed to ask
for support from
those around you.

If you have made a payment in response to a scam, contact your bank as soon as possible as they may be able to recover some of your money and will refund you in certain circumstances.

If you or someone else is in immediate danger because of a scam (for example, if they are being threatened by an aggressive doorstep caller), call the police on 999.

England & Wales

REPORT: contact **Action Fraud** on **0300 123 2040**.

ADVICE: contact **Citizens Advice** on **0808 223 1133**.

Scotland

REPORT: call **Police Scotland** on **101**.

ADVICE: contact **Advice Direct Scotland** on **0808 164 6000**.

Northern Ireland

REPORT: contact **Action Fraud** on **0300 123 2040** or call the police on **101**.

ADVICE: contact **Consumerline** on **0300 123 6262**.

You can find more general information and advice on scams on the Take Five website:
www.takefive-stopfraud.org.uk



PART ONE: STOPPING CRIMINALS FROM REACHING YOU

Mail scams

If you receive scam mail, you may want to consider reducing the amount that reaches you. Ask a friend or relative to go through your post with you and help identify any scams. Remember that scam mail can come in many forms, including lotteries, prize draws, catalogues, and clairvoyant scams. You can reduce the amount of junk and scam mail you receive by following these tips:

- Become a **Scam Marshal** and send any scam mail you receive to the National Trading Standards Scams Team to help them investigate and stop the criminals behind scams. You will receive information to help you identify scams. Sign up online at www.friendsagainstscams.org.uk or write to 'FREEPOST NTSST MAIL MARSHAL'.
- Sign up to Royal Mail's paid-for **redirection service** to have your post delivered to a trusted friend or relative. Apply online at www.royalmail.com or at a Post Office branch.
- Sign up to the **Mailing Preference Service (MPS)**. Although the MPS does not stop scam mail, it will reduce the amount of direct marketing mail that you receive. The MPS is a free service. For more information and to register visit www.mpsonline.org.uk or call **0207 291 3310**.



Scam calls

Scam calls are a common method criminals use to try to gain people's personal and financial information. The calls can be very intimidating and the criminals can apply a lot of pressure, but it's important to remember that if you're not comfortable with the call, **it's okay to hang up**. Cut out the sign at the back of this leaflet and place it near your phone to remind you. There are several options you can look at to help stop the criminals getting in contact with you:

- Look into purchasing a **call blocking unit**. These are units that connect to your landline and block scam and nuisance calls. Different brands will work in different ways and vary in how restrictive they are on incoming calls, so it's best to look at the options available and pick one that suits you.
- Many landline providers now offer options for preventing nuisance calls which are free to their customers. For more information on these, contact your landline provider or visit their website.
- Sign up to the **Telephone Preference Service (TPS)** – Although the TPS does not stop scam calls, it will reduce the amount of unwanted sales and marketing calls received. The TPS is a free service. For more information and to register, visit www.tpsonline.org.uk or call **0345 070 0707**.



Doorstep scams

To stay safe from doorstep scams, never trade with people on your doorstep. Remember, if you're not sure, don't open the door. Legitimate tradespeople will never pressure you to enter a contract straight away. Here are a few other ways that you can protect yourself from doorstep scams:

- Display a **'No Cold Calling'** sticker on your front door. Cut out the sign at the back of this leaflet or download a printable version here: www.friendsagainstscams.org.uk/NCC. You may be able to obtain a free 'No Cold Calling' sticker from your local council or local police.
- Use a **good trader scheme** to find legitimate traders. Contact your local council to find a scheme in your area.
- Install a door chain and/or a spy hole on your front door to check who is there.
- If you are expecting a trader, ask to see **identification** from them. Then phone the company they are from to check they are genuine before letting them into your home. Make sure you call using a number you know to be genuine; do not use a number they give to you.



Internet scams

With the rising threat of online scams, it's important to remember to be careful when using the internet. Criminals can create flashy, official looking websites and emails all in an aim to extract personal or financial information. Be wary of links and attachments in emails and keep your guard up – especially if you receive an email you are not expecting. Here are a few top tips:

- Keep your computer up to date – you will be better protected if you keep the operating system (such as Windows or Mac) updated. You should receive notifications when you need to update the system.
- Use the latest version of your internet browser (such as Edge, Chrome and Firefox) – this will help to provide better protection from scams, viruses and other possible threats.
- Use **security software** (for example anti-virus, anti-spyware and firewall) to protect your computer from viruses and attempts to steal your personal information. Some computers already have security software installed, or you can check www.getsafeonline.org for advice on reputable providers.



- Use a different, strong password for every online account in case one gets hacked. You can use a **password manager** to help you store your passwords securely – this means you'll only have to remember one strong master password.
- Enable **multifactor (or two-factor) authentication** on online accounts like your email. This is a safer way to log in and requires another source such as a mobile phone to authenticate that it is you logging on to your account.

You can find more information about using the internet safely on www.getsafeonline.org or search for 'How to stay safe online' at www.ageuk.org.uk for tips on avoiding online scams.

Other practical advice

It is good practice to ensure that you do not hold too much cash in your current accounts. Keep the bulk of your money in savings or deposit accounts. This means that if a criminal gains access to your current account or convinces you to make a payment, they will only be able to access a limited amount of your money.

If you are struggling to manage your financial affairs or you feel particularly concerned about scams, consider contacting your bank. Explain how and why you feel concerned about scams and ask them for help in providing additional security measures to better protect your account. The bank will then be able to offer a range of measures to support you and protect you from scams.

If you notify the bank, the bank has a duty of care to ensure you are protected.

PART TWO: HELP A FRIEND OR RELATIVE WITH THEIR FINANCES

Although we are all potential victims of financial crime and scams, there is clear evidence that criminals target lonely, older citizens, particularly those with cognitive impairment, seeing these people as 'easy' targets.

Cognitive impairment is when a person has trouble remembering, learning new things, concentrating, or making decisions that affect their everyday life. It can be caused by a number of conditions, including dementia or brain injury. Cognitive decline is when the person's cognitive ability is not going to improve but will get worse over time; it is usually not reversible.

If you have a relative or friend you care for who is experiencing cognitive decline, helping them to manage their finances, and particularly ensuring they do not become a victim of financial crime, is usually a major concern.

Remember - signing cheques on behalf of somebody else or sharing PIN numbers and internet banking passwords are, in effect, illegal. You can only legally act on behalf of somebody who lacks capacity to make their own decisions via a Lasting Power of Attorney (LPA) or if you are a court appointed deputy.



What is a Lasting Power of Attorney (LPA)?

Many people assume that because they are 'the next of kin' or a close friend that they can act on behalf of somebody with cognitive decline, especially when they lose the ability to make decisions for themselves. The technical term for this ability to make decisions is mental capacity. Unfortunately, this is not the case in law.

To legally act on behalf of a friend or relative, a valid Lasting Power of Attorney is needed (called Powers of Attorney in Scotland). A Lasting Power of Attorney (LPA) is a legal document which allows you to appoint a friend or relative to help you make decisions or to make decisions on your behalf.

How and when to apply for Lasting Powers of Attorney

Everyone over the age of 18 should consider putting LPA arrangements in place. Brain injury following an accident, a stroke, or dementia can affect us at any stage of life. Ensuring you have an LPA in place is even more important if you are diagnosed with a condition that causes cognitive decline.

If you do not have a valid and registered LPA and you lose capacity, your relatives will need to go to the Court of Protection and seek a court appointed deputy to act on your behalf. This can be a lengthy and costly process, so it is important to plan ahead and apply for an LPA.

To appoint a relative or friend as an attorney, read the guidance at www.gov.uk/power-of-attorney. You can complete the application online yourself, but you may wish to seek advice from a solicitor.

Types of Lasting Power of Attorney

There are two types of LPA. One is called a **Health and Welfare LPA (called Welfare Power of Attorney in Scotland)** and allows the nominated person ('the attorney') to speak and act on your behalf regarding your health and welfare, such as giving consent for treatment and end of life care. Health and Welfare LPAs can only come into force when you have lost capacity and you cannot give informed consent.

The **Property and Finance LPA (called Continuing Power of Attorney in Scotland)** allows the attorney to manage your financial affairs. You can specify whether:

- a) You want the attorney to act on your behalf immediately, even while you have capacity (you might prefer a relative to manage your finances).
- b) You only want the attorney to act on your behalf when you lose the mental capacity to act for yourself (for example due to dementia or cognitive decline).

Things to consider when appointing an attorney

Lasting Powers of Attorney are very important in ensuring our wishes and desires are upheld and acted upon when we are no longer able to act for ourselves.

Because they are so powerful, you must think carefully about whom you ask to be your attorney.

- Do you trust them? Are you sure they will act on your behalf in the manner you would expect and in your best interests?
- Remember you can appoint more than one person to act as your attorney. You can choose whether you want them to make decisions together or be able to act on your behalf individually.

Registering as an attorney with the bank

If you are an attorney for a person (in other words, an LPA has been drawn up asking you to act on behalf of the person – known as the donor), then you should make a branch appointment at their bank to register the LPA. Take the original or a certified copy of the LPA and proof of your ID with you to the bank. You may also be able to register over the phone.

A Property and Financial Affairs LPA will give you the legal authority to manage the accounts of the donor. The bank will set up processes and systems for you to manage and operate the accounts on behalf of the donor.

The bank will always help you with this process.

More help and advice on LPAs and managing your finances

Bournemouth University's National Centre for Post-Qualifying Social Work and Professional Practice has published guides on LPAs and on financial scamming: www.ncpqsw.com

Visit your local Citizens Advice Bureau for help and advice on managing affairs for someone else, or read the guidance on their website: www.citizensadvice.org.uk

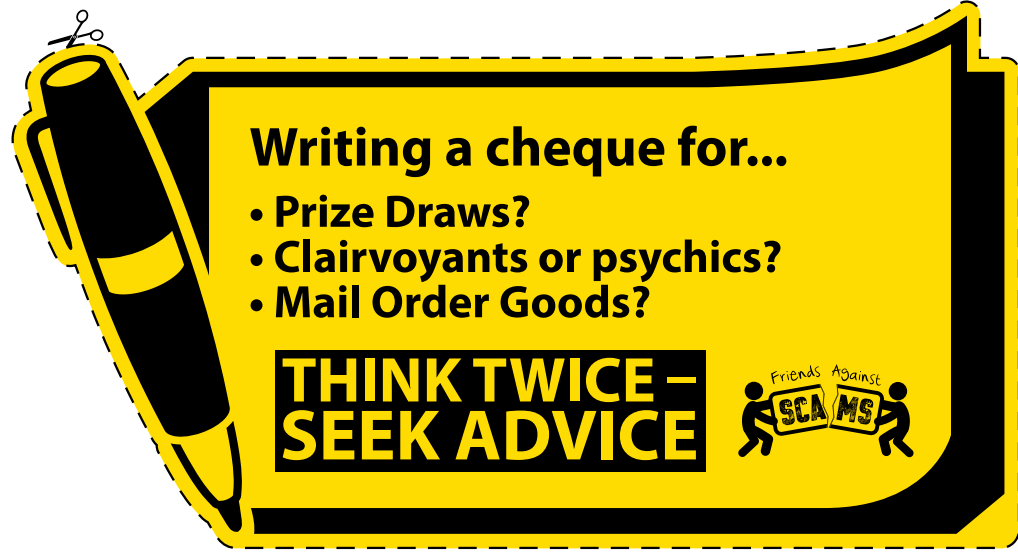
Call Age UK's advice line on 0800 678 1602; or visit your local Age UK branch. You can also find more information on their website: www.ageuk.org.uk.

The Alzheimer's Society gives advice and information on living with dementia, including how to manage your money: www.alzheimers.org.uk

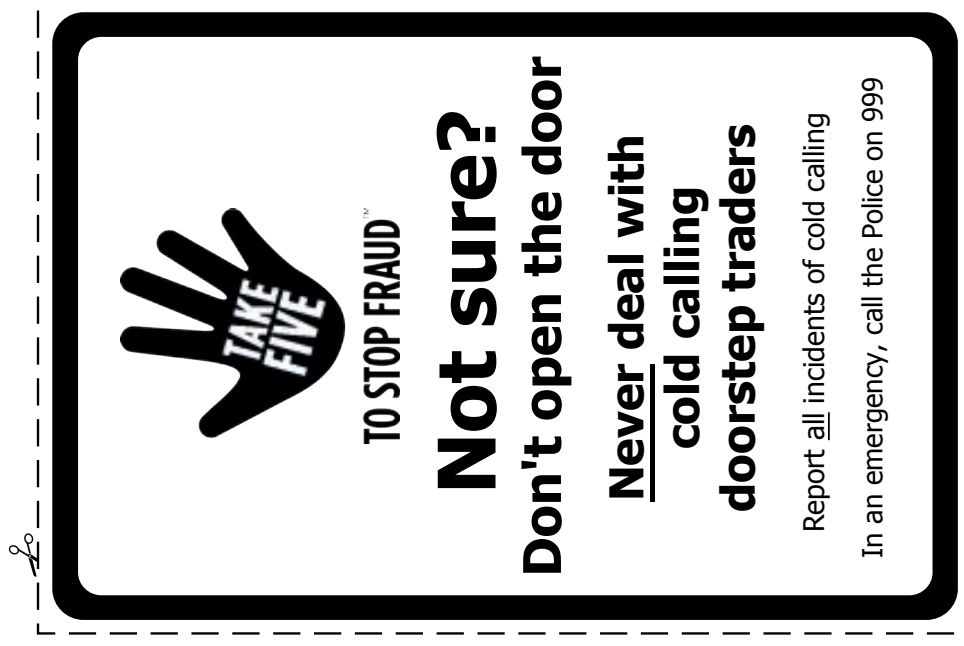
Dementia UK also has advice on living with dementia, including legal and financial aspects such as LPAs: www.dementiauk.org



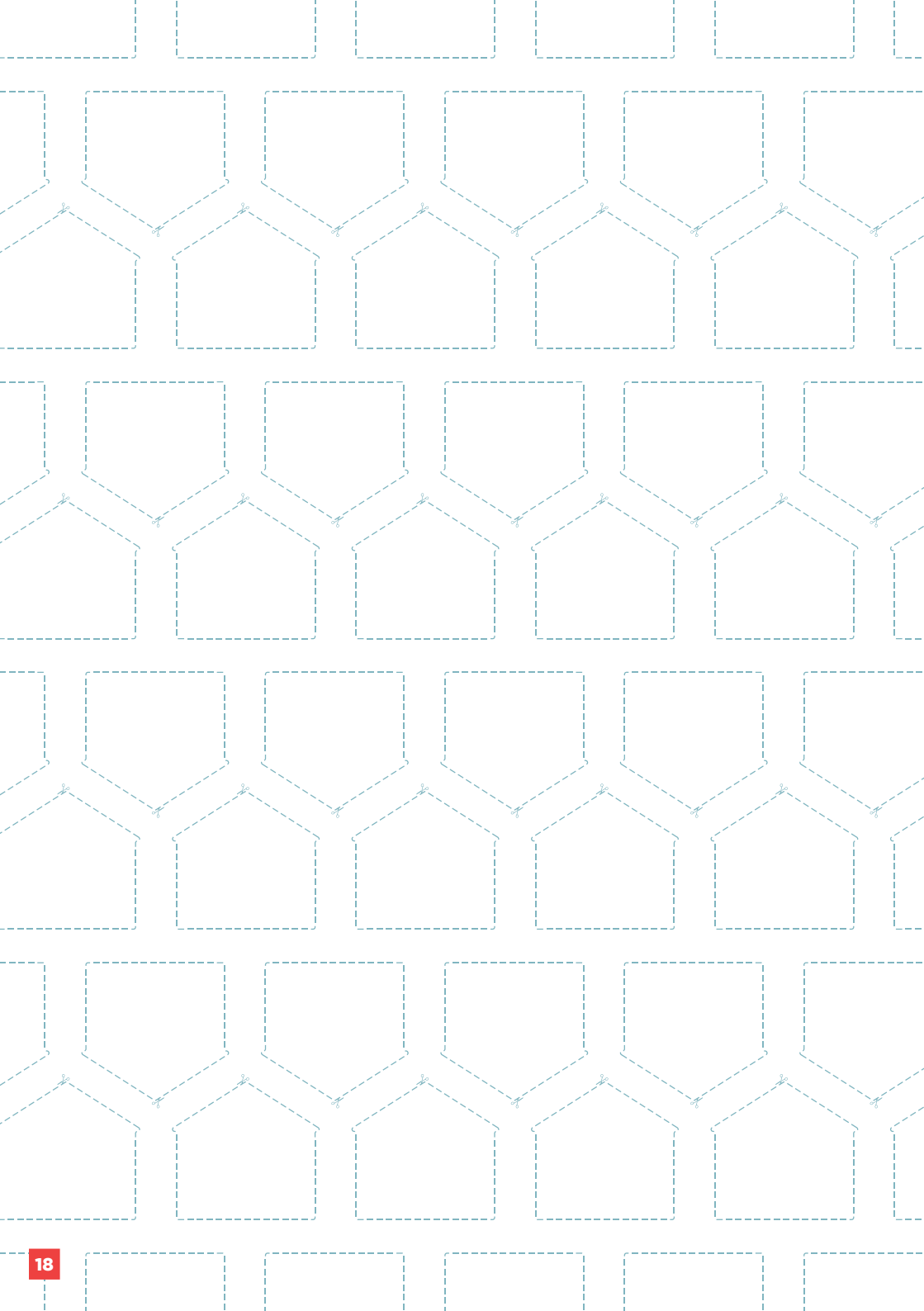
**SIGNS
FOR AROUND
THE HOME**



Stick this outside your front door



Stick this inside your front door



National Trading Standards Scams Team

Website: www.nationaltradingstandards.uk

Friends Against Scams

St Mary's House, St Leonard's Road, Eastbourne,
East Sussex, BN21 3UU.

Website: www.FriendsAgainstScams.org.uk

Email: FriendsAgainstScams@surreycc.gov.uk

National Centre for Post Qualifying Social Work and Professional Practice

Bournemouth University, 4th Floor, Royal London House,
Christchurch Road, Bournemouth, BH1 3LT

Website: www.ncpqsw.com

Email: pqsw@bournemouth.ac.uk

