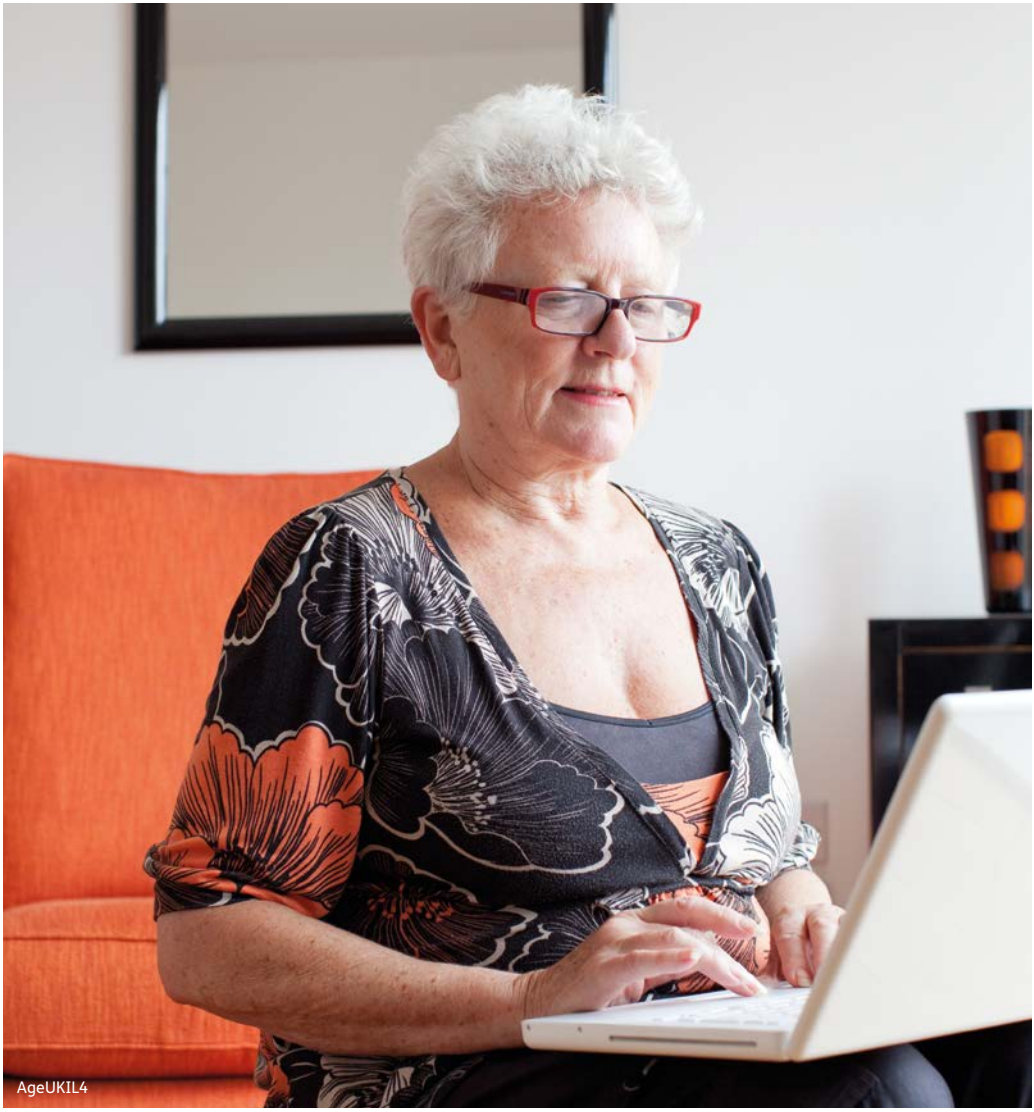
Internet security

Staying safe online

Age UK
Love later life



AgeUKIL4

Information and advice you need to help you love later life.

We're Age UK and our goal is to enable older people to love later life.

We are passionate about affirming that your later years can be fulfilling years. Whether you're enjoying your later life or going through tough times, we're here to help you make the best of your life.

Our network includes Age Cymru, Age NI, Age Scotland, Age International and more than 160 local partners.

Date of publication: June 2017. © Age UK 2017
Next review date: June 2019

Contents

What this guide is about

For many people the internet has made life easier and is an excellent source of information. But it's important to use the internet safely and protect any device that connects to the internet.

You may not realise it, but you already have a lot of the skills and intuition to stay safe online. All you have to do is apply the same common sense you use in everyday life. For example, you wouldn't open your front door and invite a stranger into your home, so it makes sense not to open email attachments from someone you don't know. Being aware of the risks that come with using the internet and taking steps to avoid them means you can enjoy the internet safely.

This guide looks at some common internet and computer scams, what you can do to protect yourself online, and how you can protect your mobile phone and computer. Words in bold may be unfamiliar to you, so we've included a glossary on pages 21–23.

Age UK offers computer and internet training for older people. Visit the 'Work & learning' section on our website to find information about our computer training courses, or ask your local Age UK about your nearest training opportunities. To find contact details for your local Age UK, call Age UK Advice on 0800 169 65 65, or go to www.ageuk.org.uk

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

Key

This symbol indicates who to contact for the next steps you need to take.

Email encounters

Email has made it easier to communicate with family and friends and stay informed about the latest products and services. Unfortunately, fraudsters may sometimes use email to spread **viruses,** obtain personal information or trick people into buying products. Your email accounts are usually protected so that suspicious emails are blocked out without you having to do anything. However, it's still important to be aware of the common types of email scams so that you can protect your personal information.

Spam

Spam, or junk mail, is usually from a person or organisation trying to sell something. Most email providers (such as Gmail Yahoo Mail or Hotmail) have spam filters or anti-spam protection to automatically block emails from untrustworthy sources.

Common types of spam include:

- advertisements from a company
- an email telling you about a scheme to make you rich
- an email warning you of a virus
- an email encouraging you to send the email onto more people.

These may even come from an email address that you recognise, such as a friend or family member, as sometimes accounts can be **hacked** into and fake emails sent out to all of that person's contacts.

Phishing

Phishing is when criminals send bogus emails to thousands of people, in an attempt to get you to disclose private information (e.g. your login or password) or to infect your device with viruses. These emails may look as though they come from reputable organisations, such as banks, credit-card companies, online shops and IT companies, but they are actually from fraudsters.

Common types of phishing scams can be:

- from your 'bank' asking you to update your security information (e.g. your password) or your account will be closed
- from a well-known company (e.g. PayPal, Amazon) asking you to update your account details or install a programme on your device
- from a government agency (e.g. HMRC) telling you about a rebate or penalty
- an email saying you have won some kind of prize, lottery or inherited a large amount of money
- an email supposedly by someone you know asking for money because they are stranded somewhere or need medical assistance
- an email with a link or document attached for you to click on or open. If you click on the link or document, a virus may be released onto your device so fraudsters can get access to your personal information.

How to recognise spam and phishing emails

- The sender's email address may look official but it is not the actual email address of the bank or company. Always check with your bank if you are unsure.
- The email does not use your proper name, but instead starts with a general greeting like 'Dear customer'.
- There's a sense of urgency, for example threatening that unless you act immediately, your account will be closed or a deal will expire.
- It may contain a link to a website that looks very similar to the company's real one but is actually a fake site asking for your personal details. The link or site may be slightly different to the official website, so check it carefully. Be aware that you can be taken to a fake website even if the link appears to be correct.
- There may be a request for personal information, such as your username, password or bank details.
- There may be a request for money, for example for processing your prize, or for helping someone in need.
- There may be a document or link to open and either no message or some short text saying 'Check this out' or 'See what I found' without further explanation.
- The email may have errors in its spelling or grammar, or be written in an unusual style.

What to do if you receive a suspicious email

- If in doubt delete it without opening it. Do not open emails from strangers or emails that you suspect may be a scam.
- Do not open an email link or document **attachment** unless you are sure it's safe.
- Do not reply to spam or suspicious emails, even to say no, as this demonstrates that your email address is active so they may contact you again.
- Banks and other financial institutions never ask for personal information in an email. If you receive a suspicious email claiming to be from your bank, contact your bank directly by phoning them or typing their web address into your **browser** (not by following the link in the email).
- If it's about account information, phone the organisation directly to ask about the email, using the phone number found on their official website.
- Don't panic if you get an email that has a sense of urgency and threatens to close your account. Take your time to check the details first before reacting.
- If you receive a strange email from a friend or family member, send them a separate email or call them to ask if it's genuine.

Report suspicious emails

You can report phishing emails to your email provider or Action Fraud (see page 25).

what next?

Visit the 'Protecting Yourself' section on the Get Safe Online website for more information and tips on email scams (see page 25). Learn My Way also offer free online courses, including email basics and how to identify email scams (see page 26).

Computer scams

Beware of a common scam. The fraudsters phone you claiming to be from a well-known IT (information technology) firm, asking you to follow a few simple instructions to get rid of a virus, update your software or fix another issue with your computer. If you do as they ask, they will upload software called **spyware** onto your computer, which allows them to access any personal details you have stored on your computer.

Legitimate IT companies never contact customers in this way. Never respond to a phone call from someone claiming that your computer has a virus. If you get a call like this, hang up straight away.

Report a computer scam

You can report a computer scam to Action Fraud (see page 25).

what next?

See our free guide *Avoiding scams* for more information on different types of scams and how to avoid them.

Passwords

Passwords are the most common way to prove your identity online, so it's very important to make sure you have strong passwords that can't be easily guessed.

Avoid weak passwords

Weak passwords are made up of common sets of letters or numbers. Examples of weak passwords that are used a lot include:

- password
- 123456
- password123

Choose a strong password

A strong password should:

- be at least 8 characters long
- include a combination of upper and lower case letters
- include some numbers and keyboard symbols such as & or !
- not include personal information, such as your name, date of birth or any family member's details.
- not include common words like 'password'.
- not be too difficult to remember.

If passwords with numbers and symbols are too hard to remember, using three random words together can make a stronger password, as long as those words don't contain your personal information.

Choose different passwords

Use different passwords for different websites or accounts. Using one password for all accounts is a potential security risk because if a stranger gets access to (or hacks) your account on one site, they will be able to log in to all the accounts that share that password.

Be careful writing down your passwords

Never write down your password. If you need a written reminder, try to write a hint that only you'll understand, rather than the actual and complete password itself.

If you do write anything down, keep that information somewhere safe away from your computer. It's best to keep it in an unmarked notebook so it won't be obvious to other people what information is inside.

Password managers

Some internet browsers have built-in password managers. This is a tool that remembers your passwords for different sites and fills them in for you automatically.

When you log in to a website for the first time, the password manager will ask if you want it to remember the password. You have the choice if you want it to or not. It can save time to use this function, but it will only work on your own computer.

If you use a password manager and you share your computer with someone else, they will be able to access all your log-in details through the password manager. Make sure that your computer is only used by people you trust. Don't use the password manager on a public computer, for example in a library, so that strangers can't access your account.

what next?

Visit the 'Protecting Yourself' section on the Get Safe Online website for more tips on choosing a strong password and keeping your passwords safe (see page 25).

Online shopping and banking

The internet can offer useful ways to do your shopping and manage your money from home. More and more people are discovering that it's quick and convenient, and can even lead to some savings.

If you make purchases or bank online, make sure you protect your financial information. Use a website that's secure when entering card information. This ensures that the information you send can't be read by anyone else.

How to spot a secure website

- The website address should begin with 'https://'. The 's' stands for 'secure'.
- If the address bar is green, this is an additional sign that you're using a safe website.
- Look for a padlock symbol in the browser next to the website address. Don't be fooled by a padlock that appears on the webpage itself.
- Websites that offer secure payments and other financial transactions, such as banking, need a security certificate. To view it, click on the padlock symbol to check that the seller is who they say they are. The certificate should be current and registered to the right address. However, the padlock isn't an absolute guarantee of safety, so be cautious if you have any doubts.

Tips for shopping and banking online safely

- You'll never be asked for your card PIN (personal identification number) but you may be asked to provide the security number for your debit or credit card, referred to as 'CVV', 'CVC' or 'CVV2' (Card Verification Value). This is the last three digits on the reverse of your card. If you have an American Express branded card, the CVV is 4 digits and is on the front of your card.
- If you get a **pop-up** message warning you about a website's security certificate, be very cautious. If you continue, you may be redirected to a fake website, designed to let somebody else read the information you are sending, such as log-in details.
- Use a strong password that can't easily be guessed by others (see page 8).
- Use online retailers that have a good reputation, either as high-street shops or as established online stores.
- If a deal looks too good to be true, it probably is. Be cautious of anything offered in an email you did not request. You could do an internet search to see whether anyone else has had problems or if it's a well-known scam.
- Check where the seller is located. Don't assume that a seller is based in the UK just because their web address has 'uk' in it. The law says that the seller must provide you with their full contact details. If you buy from a seller or company based outside the EU, it can be more difficult to enforce your rights and problems can be harder to sort out.
- There may also be added or hidden costs, such as VAT or additional postage for overseas transactions. To find more information on buying from sellers based in other EU countries, visit the UK European Consumer Centre website (see page 26).

- Always use a credit card for internet transactions, or check to see if your debit card provider offers any protection. If your purchase costs more than £100 and you use a credit card, the seller and your card company are equally responsible if anything goes wrong. Be aware that there is sometimes a card handling fee when you pay with your credit card. Always check how much this is before completing your transaction.
- Many banks offer free **anti-virus** software or browser security products – check if your bank offers this.
- After you've finished using a secure site always make sure you log out. That way anyone using the computer after you won't be able to access your personal information.

what next?

See our free guide *Avoiding scams* for information on how to protect yourself. Learn My Way offers free online courses, including getting started with online shopping, online payment methods and consumer rights (see page 26).

After you've finished using a secure site always **make sure you log out**. That way anyone using the computer after you won't be able to **access your personal information**.

Social networking

Social networking websites are online communities where you can connect with people who share your interests. You can create a **profile** describing yourself, exchange public and private messages and join groups that interest you.

They're a great way to keep in touch with family and friends, make new friends, share your photos, find out about events and much more. Facebook (www.facebook.com) and Twitter (www.twitter.com) are among the most popular sites.

Social networking sites can be targets for people who want to steal personal information, but it's easy to stay safe by following a few sensible guidelines.

- Be aware of who can see your profile. Most social networks allow you to choose who can see your profile and how much they can see, but you may have to change your settings to make it private.
- Be wary of publishing any information that identifies you, such as your phone number, photos of your home, your address, date of birth or full name.
- If possible, pick a username that doesn't include any personal information. For example, avoid using 'annajones1947'.
- Set up a separate email account that doesn't use your real name to register with the site. If you don't want to use the site any more, you can simply stop using that email account.

- Use a strong password that is different from the passwords you use for other accounts (see page 8).
- Be cautious with people you've just met online who ask you to reveal personal information or who want to meet you very quickly.
- Be on your guard against phishing scams (see page 4).

what next?

Visit the Get Safe Online website (see page 25) for more information about using social networking sites securely. Learn My Way offers free online courses, including protecting yourself when using social media (see page 26).

Social networking sites can be targets for people who want to steal personal information, but **it's easy to stay safe**.

Protect your computer

Protecting your computer from harmful **malware** or viruses is simple, just follow the tips below.

Install anti-virus software

Viruses are malicious programs that can spread from one computer to another by email or through websites. They can display unwanted pop-up messages, slow your computer down and even delete files. Remember to check which type of software you need, as it may vary depending on whether your computer uses Windows software or is an Apple computer.

Anti-virus software helps to find, stop and remove these malicious viruses.

Install anti-spyware software

Spyware is an unwanted program that runs on your computer. It allows unwanted adverts to pop up, tracks your online activities and can even scan your computer for private data such as credit card numbers. It can make your computer slow and unreliable and make you a target for online criminals.

Installing **anti-spyware** software helps to protect your computer from these threats.

It may seem like you need a lot of software to protect yourself from online risks, but it's actually very easy. You can buy a complete package that includes everything you need, or get effective free software such as AVG (http://free.avg.com) or Avast (www.avast.com). These work on both Windows computers and Apple computers.

Online threats change constantly so once your software is installed, keep it up to date when prompted. This ensures that you have the highest level of protection.

Keep your operating system updated

The **operating system** is the main software program on your computer, which manages all the other programs on it – the most common systems are Microsoft Windows and Mac OS. Whichever operating system you have, keep it updated as this will give you better protection. You should receive notifications when new updates are available but you can also update your software manually.

Protect your wireless network

If you use wireless internet at home, you will have a wireless **router**. You need to protect your **wireless network** (also known as wi-fi) so that people living nearby can't access it. Read the instructions that come with your router to find out how to set up a 'key' – a type of password – so that no one else can access the internet through your router.

what next?

You can find step-by-step explanations and advice on protecting your computer on the Get Safe Online website (see page 25).

Protect your tablet and your mobile phone

Tablets (e.g. iPad) and **smartphones** can now be used to do things like check emails, shop and bank online or explore the internet.

Tablets and smartphones need protecting just like computers do. That's because they can still be infected with viruses or spyware. Just like on computers, viruses on your tablet or smartphone could be used to get your personal details, slow your device down or spread viruses to other tablets or computers.

You can download anti-virus and anti-spyware protection for tablets and phones. These are often referred to as **apps** (applications), which is just another term for software. The best protection for your device may vary depending on the type of phone or tablet you have. If you're unsure about which is best, you could ask your mobile phone provider, pop into a local phone shop or look online for more information. A lot of good anti-virus protection for phones and tablets is free and can be downloaded online.

Some highly rated anti-virus apps, which are free, are:

- Avast mobile security (visit www.avast.com)
- Kaspersky internet security (visit www.kaspersky.co.uk)
- Norton mobile security (visit uk.norton.com/norton-mobile-security)

These apps work on phones and tablets that use Windows, Android and Apple products.

Download the latest software and app updates

Your tablet or mobile phone may prompt you when there is a new software or app update. This will give your device the latest security protection and may provide some new features.

Password protect your device

You should also password-protect your phone or tablet, to make sure that only you, or people you trust, can use it. Password access is easy to set up, just follow the instructions that come with your device.

what next?

Visit Get Safe Online to find more information on protecting your smartphone or tablet (see page 25). See our free guide *Avoiding scams* for information on telephone scams, including text messages.

Tablets and smartphones **need protecting** just like computers do. That's because they can still be **infected with viruses** or spyware.

Being aware of the risks that come with **using the internet** and taking steps to avoid them means you can **enjoy the internet safely**.

Glossary

Anti-spyware
Helps protect your computer against pop-ups, slow performance and security threats caused by spyware and other unwanted software.

Anti-virus
Software that detects and prevents known viruses from attacking your computer.

Apps (applications)
A type of computer program that you can download for your computer, tablet or mobile phone. There are hundreds of different apps available, some for free, which do lots of different things, from playing games and puzzles, to helping you remember to take your medications, or allowing you to access your bank account.

Attachment
Files, such as photos, documents or programs that are sent along with an email.

Browser
The computer software or app you use to access the internet. Examples include Internet Explorer, Google Chrome and Safari.

Hack
An attempt to gain unauthorised access to a computer or account.

Malware
Malware is short for 'malicious software'. A general term used to refer to hostile or intrusive software.

Operating system
The software that manages different programs on a computer.

Phishing
An attempt at identity theft in which criminals direct users to a counterfeit website to trick them into disclosing private information, such as usernames or passwords.

Pop-up
A small window that suddenly appears (or 'pops up') on a webpage, usually an advertisement or an alert.

Profile
A description that may include your personal details and is used to identify you on a social networking website. This can be set as public (viewed by everyone) or private (only viewed by certain people).

Router
A device that connects your computer to a broadband-enabled telephone line and emits your home internet signal.

Smartphone
A mobile phone which, as well as making calls and sending texts, can connect to the internet, send emails, and do a number of other functions like a computer.

Social networking website
An online community where you can connect with friends, family and other people who share your interests.

Spam
A commercial email that you did not request, also known as junk mail.

Spyware
An unwanted program that runs on your computer, which can make it slow and unreliable or even make you a target for online criminals.

Tablet
A larger handheld device with a touchscreen which can connect to the internet and be used as a portable computer.

Viruses
Programs that spread from one computer to another by email or through malicious websites. They can slow your computer down, display unwanted pop-up messages and even delete files.

Wireless network
Also known as wi-fi, this is a way for your computer to connect to the internet without using wires or cables.

Useful organisations

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

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

Call Age UK Advice to find out whether there is a local Age UK near you, and to order free copies of our information guides and factsheets.

In Wales, contact
Age Cymru: 0800 022 3444
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

The evidence sources used to create this guide are available on request. Contact **resources@ageuk.org.uk**

Action Fraud

Investigates reports of phishing emails and online fraud. Report phishing emails directly via their website.

Tel: 0300 123 2040
www.actionfraud.police.uk

BBC Webwise

Free online information, articles and videos about using the internet.

www.bbc.co.uk/webwise

Citizens Advice Consumer Service

Provides information and advice on consumer issues by telephone and online. Offers tips on recognising email scams.

Tel: 0345 404 0506
(0345 404 0505 for a Welsh-speaking adviser)
www.citizensadvice.org.uk/consumer

In Northern Ireland, contact **Consumerline**
Tel: 0300 123 6262
www.nidirect.gov.uk/consumerline

Digital Unite

Helps older people learn about computers and the internet. It has a network of tutors across the UK who offer one-to-one tuition for a fee. There are also useful step-by-step instructions for using the internet and computer on its website.

Tel: 0800 228 9272
www.digitalunite.com

Get Safe Online

Free advice about using the internet safely.

www.getsafeonline.org

GOV.UK
Government website offering practical information and advice to the public.

www.gov.uk

In Northern Ireland, visit **NI Direct** at www.nidirect.gov.uk

Information Commissioner's Office
Provides information about data protection.

Tel: 0303 123 1113
ico.org.uk

Learn My Way
A website of free online courses for beginners on using a computer, browsing the internet, sending an email and finding work online.

www.learnmyway.com

Online Centres Network
Provides access to computers and the internet, and helps people gain basic digital skills. Use the 'find a centre' facility to locate your nearest Online Centre.

Tel: 0114 349 1666
www.onlinecentresnetwork.org

UK European Consumer Centre
The UK European Consumer Centre provides advice on sorting out problems with traders based in other EU countries.

Tel: 01268 886 690
www.ukecc.net

Can you help Age UK?

Please complete the donation form below with a gift of whatever you can afford and return to: **Freepost Age UK Supporter Services**. Alternatively, you can phone 0800 169 87 87 or visit www.ageuk.org.uk/donate If you prefer, you can donate directly to one of our national or local partners. Thank you.

We'd † like to let you know about the vital work we do for older people, our fundraising appeals and opportunities to support us, as well as the Age UK products and services you can buy.

Personal details

Title:	Initials:	Surname:

Address:

Postcode:

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

☐ Please tick here if you **do not** wish to receive communications by post.

You can change your mind at any time by telephoning us on 0800 169 8787 or by writing to Supporter Services at the registered address below.

Your gift

I would like to make a gift of: £

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

Card payment

I wish to pay by (please tick) ☐ MasterCard ☐ Visa ☐ CAF CharityCard ☐ Maestro ☐ American Express

Signature **X**

Expiry date /

Gift aid declaration

☐ Yes, I want Age UK and its partner organisations* to treat all donations I have made for the four years prior to this year, and all donations I make from the date of this declaration until I notify you otherwise, as Gift Aid donations. I am a UK tax payer and understand that if I pay less income tax and/or capital gains tax than the amount of Gift Aid claimed on all my donations in that tax year it is my responsibility to pay any difference.

Date__/__/__ * Age Cymru, Age Scotland and Age NI

age UK
Love later life

† We, includes the charity, its charitable and trading subsidiaries, and national charities (Age Cymru, Age Scotland and Age NI). Age UK is a charitable company limited by guarantee and registered in England (registered charity number 1128267 and registered company number 6825798). The registered address is Tavis House, 1-6 Tavistock Square, London WC1H 9NA. **Age UK provides a range of services and your gift will go wherever the need is the greatest.**

MXAQ17CA01C028

Supporting the work of Age UK

Age UK aims to enable all older people to love later life. We provide vital services, support, information and advice to thousands of older people across the UK.

In order to offer free information guides like this one, Age UK relies on the generosity of its supporters. If you would like to help us, here are a few ways you could get involved:

1 **Make a donation**
To make a donation to Age UK, simply complete the enclosed donation form, call us on **0800 169 8787** or visit **www.ageuk.org.uk/get-involved**

2 **Donate items to our shops**
By donating an unwanted item to one of our shops, you can help generate vital funds to support our work. To find your nearest Age UK shop, visit **www.ageuk.org.uk** and enter your postcode into the 'What does Age UK do in your area?' search function. Alternatively, call us on **0800 169 8787**

3 **Leave a gift in your will**
Nearly half the money we receive from supporters come from gifts left in wills. To find out more about how you could help in this way, please call the Age UK legacy team on **020 3033 1421** or email **legacies@ageuk.org.uk**

Thank you!

What should I do now?

For more information on the issues covered in this guide, or to order any of our publications, please call Age UK Advice free on **0800 169 65 65** or visit **www.ageuk.org.uk/workandlearning**

Our publications are also available in large print and audio formats.

The Age UK Group offers a wide range of products and services specially designed for people in later life. For more information, please call **0800 169 18 19**.

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