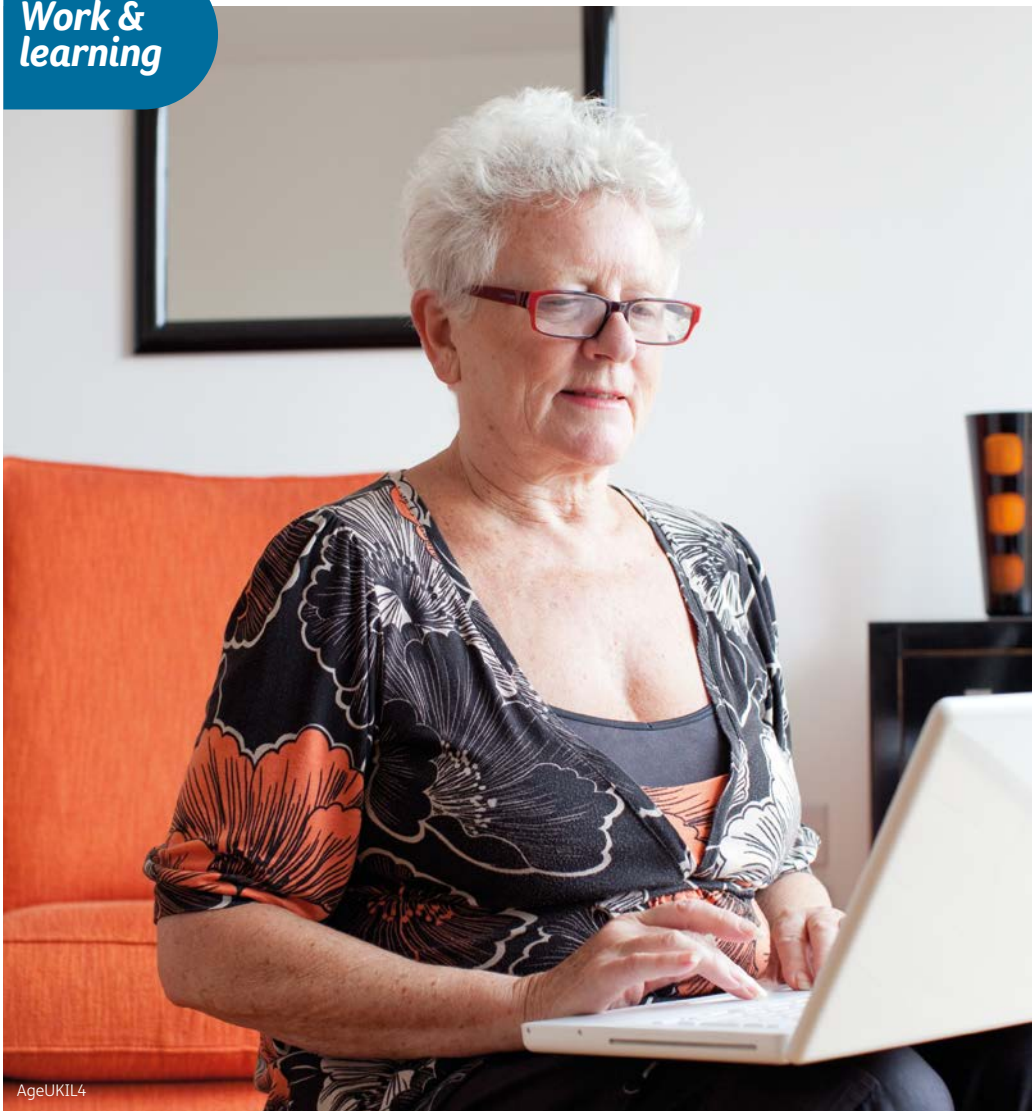
Internet security

Staying safe online

Age UK
Love later life

Work & learning



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: December 2015 © Age UK 2015

Contents

What this guide is about

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 the steps to avoid them means you can enjoy the internet safely.

This guide looks at how to protect yourself online and how to protect your computer. Words in bold may be unfamiliar to you, so we've included a glossary on pages 22–23.

Age UK offers computer and internet training for older people. Visit our website at www.ageuk.org.uk and click 'Technology & internet' in the 'Work & learning' section, or ask your local Age UK about training opportunities near you. To find your nearest Age UK call 0800 169 65 65.

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

Key

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

Email encounters

Have you received a suspicious email? It may claim to be from your bank, asking you to update your security information. Or maybe it's offering you something that sounds too good to be true. If you have received emails like these, you may have been the target of a common scam called '**phishing**'.

Phishing is where criminals send bogus emails to thousands of people, in an attempt to get you to disclose private information. 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:

- From your 'bank' asking you to update your information or your account will be closed.
- From a well-known software company asking you to update your account details or install a programme on your computer.
- An email saying you have won some kind of lottery or inherited a large amount of money.
- An email supposedly from someone that you may know asking for money because they are stranded somewhere or need medical assistance.

You may also get unsolicited emails with a link or document attached for you to open or click on. These are called '**spam**' or 'junk mail'. 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.

How to recognise phishing and spam 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 what address they use.
- 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.
- 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 will 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.

Top things to remember:

- 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).
- Do not open a link or document in an unsolicited email.
- Do not reply to unsolicited emails, even to say no, as this demonstrates that your email address is active and they may contact you again.
- If in doubt – delete it without opening it.
- If it is about account information, phone the organisation directly to ask them, using the phone number found on the 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.

Most email packages, including free email accounts from providers such as Yahoo! Mail, Hotmail or Gmail, have **spam** filters built in which can block unwanted emails.

You can report phishing emails to your email provider or Action Fraud (see page 25). You could also forward the email to the organisation it claims to be from so they can take note of it.

what next?

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

Computer scams

Beware of a common scam. The fraudsters phone you claiming to be from a well-known IT firm, asking you to follow a few simple instructions to get rid of a **virus** or update your software. If you do as they ask, they will upload software called **spyware** onto your computer, which will allow them to access any personal details you have stored on your computer. 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. Legitimate IT companies never contact customers in this way.

what next?

You can find out more about other scams in our free guide *Avoiding scams*.

Never respond to a phone call from someone claiming that your computer has a virus.

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.

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

- password
- 123456
- password123

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 !

Follow these tips to create a strong password:

- Avoid using personal information, such as your name, date of birth or common words like 'password'.
- Make sure that you don't make your password too difficult to remember.
- Use different passwords for different websites. Using one password for all accounts is a potential security risk because if someone hacks into your account on one site, they will be able to log in to all the accounts that share that password.
- Recent advice suggests that using three random words together can make a stronger password, as long as those words don't contain your personal information.

For useful tips on how to create a strong password, see www.microsoft.com/en-GB/security/online-privacy/passwords-create.aspx

It used to be advised never to write down your password. But as people get more online accounts with different and complex passwords they can become harder to recall. If you need to write down your passwords, try to write only a reminder or hint 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 automatically for you.

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 be time-saving to use this function, but it will only work on your computer. If you use someone else's computer, you will need to remember your passwords for any accounts you want to access.

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.

If you make purchases or bank online, make sure you protect your financial information.

Online shopping and banking

The internet can offer a useful way 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 secure website when entering card information. This ensures that the information you send can't be read by anyone else.

Here are some ways 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 where the website address is. Don't be fooled by a padlock that appears on the web page 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 and that their certificate is current and registered to the right address. However, the padlock isn't an absolute guarantee of safety, so err on the side of caution if you have any doubts.

Try these tips for shopping and banking online safely:

- Be aware that you will never be asked for your card pin number but you may be asked to provide the security number for your debit or credit card. This is also referred to as a 'CVV2 code' and can be found on the reverse of your card where the signature box is. It's the last 3 digits of the number on the back.
- If you get a pop-up message warning you about a website's security certificate, be very cautious indeed. 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 established online stores.
- If a deal looks too good to be true, it probably is. Be cautious of anything offered in an unsolicited email. 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 harder 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 website of the UK European Consumer Centre (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 can't access your personal information.

what next?

See our free guide *Avoiding scams* for information on how to protect yourself or visit www.getsafeonline.org for more 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 are 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, 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.
- Pick a username that doesn't include any personal information. For example, 'joe_glasgow' or 'annajones1947' would both be bad choices.
- 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 of people you have 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 3).

what next?

For more information on relationship scams see our free guide *Avoiding scams*.

Social networking websites are a great way to keep in touch with family and friends.

It may seem like you need a lot of software to protect yourself from online risks, but it's actually very easy.

Protect your computer

Protecting your computer from **malware** 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/free-antivirus-download). These work on both Windows computers and Apple computers.

For computers that use Windows 7 or above, there is built-in anti-spyware software called Windows Defender.

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

Turn on your firewall

A **firewall** is a protective barrier between your computer and the internet. It will stop some viruses getting through and will prevent anyone connecting to your computer without your permission. Most computers come with a firewall which is usually switched on automatically, but check to make sure that it is running.

Keep your operating system updated

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

If you use Windows, go to the Windows Update site at http://windowsupdate.microsoft.com. There are instructions on the site that will enable your computer to automatically download and install updates as they become available. These are free.

Protect your wireless network

If you use wireless internet at home, you will have a wireless **router**. You need to protect your **wireless network** 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 all of the above at www.getsafeonline.org

Once your software is installed, keep it up to date when prompted.

Protect your tablet and your phone

Mobile phones and **tablets** can now be used to do things like check emails, shop and bank online or explore the internet.

Tablets are small handheld devices with a touchscreen, although you can get a keyboard to attach to them if you prefer to type on one. **Smartphones** are mobile phones that have touchscreens and the ability to connect to the internet. A lot of people now use tablets or phones instead of computers.

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 what 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
- Kaspersky internet security
- Norton mobile security.

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

You should also consider password-protecting 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?

Find more information on protecting your smartphone or tablet at www.getsafeonline.org

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 software program that you can download for your computer, tablet or phone. There are hundreds of different apps available, some for free, which do lots of different things.

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

Firewall
Firewalls prevent unauthorised access to your computer over the internet.

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

Router
A device that connects your computers 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 be used to browse 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
Unsolicited commercial email, 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 handheld device with a touchscreen which can 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
Usually shortened to 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** by calling
Silver Line Scotland: 0800 470 8090 (This is a partnership between The Silver Line and Age Scotland)
www.agescotland.org.uk

Action Fraud
Investigates reports of phishing emails and online fraud.

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

BBC Webwise
Free online information and training 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
(or 0345 404 0505 for a Welsh-speaking adviser)
www.adviceguide.org.uk

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

Computer Courses Wales
A website run by Digital Communities Wales that you can search to find local computer courses.

http://computercourses.wales/

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 is also useful information 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

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

UK Online Centres
Use the 'find a centre' facility to locate your nearest UK online centre for access to computers and the internet.

Tel: 0800 771 234
www.ukonlinecentres.com

Can you help Age UK?

Please complete the donation form below with a gift of whatever you can afford and return to: Age UK, Tavis House, 1–6 Tavistock Square, LONDON WC1H 9NA. 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.

Personal details

Title: | Initials: | Surname:

Address:

Postcode:

Tel: | Email:

By providing your email address and/or mobile number you are agreeing to us contacting you in these ways. You may contact us at any time to unsubscribe from our communications.

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

(Maestro only)

Signature **X**

Expiry date / Issue no. (Maestro only)

Gift aid declaration

☐ (please tick) 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 confirm I pay an amount of income tax and/or capital gains tax at least equal to the tax that the charity will reclaim on my donations in the tax year. Date: ___/___/___ (please complete). *Age Cymru, Age Scotland and Age NI

age UK
Love later life

The Age UK Group may use the information you have supplied to tell you about our other charitable services or to ask you to support our work. Age UK (registered charity no 1128267) comprises the Charity, its group of companies and national partners (Age Cymru, Age Scotland & Age NI). If you would prefer not to hear from us do let us know by phoning 0800 107 8977 or by writing to us at our registered address. The registered address is Tavis House, 1–6 Tavistock Square, London WC1H 9NA.

MXXX15CA07C009

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 following Age UK information guides may be useful:

- *Avoiding scams*
- *Save energy, pay less*
- *Staying safe*

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**.