Internet security

Staying safe online

Age UK
Improving later life

Work & learning

AgeUKIL4

We are Age UK.

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

This information leaflet has been prepared by Age UK and contains general advice only, which we hope will be of use to you. Nothing in this leaflet should be construed as the giving of specific advice and it should not be relied on as a basis for any decision or action. Neither Age UK nor any of its subsidiary companies or charities accepts any liability arising from its use. We aim to ensure that the information is as up to date and accurate as possible, but please be warned that certain areas are subject to change from time to time. Please note that the inclusion of named agencies, websites, companies, products, services or publications in this information leaflet does not constitute a recommendation or endorsement by Age UK or any of its subsidiary companies or charities.

Every effort has been made to ensure that the information contained in this leaflet is correct. However, things do change, so it is always a good idea to seek expert advice on your personal situation.

Date of publication: February 2013 © Age UK 2013

FSC
www.fsc.org
MIX
Paper from
responsible sources
FSC® C013983

Contents

We are grateful to Get Safe Online for their generous input to this guide.

Introduction

You may not realise it, but you already have the skills and intuition to stay safe online. All you have to do is apply the 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 an email from someone you don't know.

You have a lifetime's experience of judging character, weighing up whether an offer looks as if it's good value and genuine, and dealing with cold callers at your door. Once you learn how to apply these rules to the internet, you can relax in the knowledge that you have done all you can to protect yourself.

This leaflet looks at both how to protect yourself online and how to protect your computer. We recommend that you read it alongside our free guide *Making the most of the internet*, especially if you are new to using a computer. Words in bold may be unfamiliar to you, so we've included a glossary on pages 14–15.

Age UK works with the Digital Inclusion Network, which specialises in computer and internet training for older people. To find out whether there is a course in your area, 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.

Throughout this leaflet you will find suggestions for organisations that can offer further information and advice about your options. Their contact details can be found in the 'Useful organisations' section (see pages 16–18). Contact details for organisations near you can usually be found in your local phone book. If you have difficulty finding them, your local Age UK should be able to help (see page 16).

As far as possible, the information given in this leaflet is applicable across the UK. This information leaflet has been prepared by Age UK and Get Safe Online.

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? Perhaps it claims 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. These are common problems, but fortunately they're easy to deal with.

If you have received emails like these, you may have been the target of a common scam called **'phishing'** – where criminals send bogus emails to thousands of people, in an attempt to get you to disclose private information. These emails look as though they come from reputable organisations, such as banks, credit-card companies, online shops and IT companies, but they are actually from criminals. The emails will direct you to a website that looks like the real organisation's site but is, in fact, a fake site designed to trick you into entering personal information, such as a password or credit-card number. Banks and other financial institutions never ask for personal information in an email.

These emails often show some of the signs listed below.

- The sender's email address doesn't match the real organisation's website address.
- The email does not use your proper name, but uses 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.

- A link to a fake website, which may look very similar to the proper address. However, a single character in the web address may be different, taking you to another website that appears to be the reputable company's website but is actually a fake.

- A request for personal information, such as your username, password or bank details.

- The email comes out of the blue and is from a company that you weren't expecting to hear from. You can reduce the number of unwanted emails (also known as **'spam'**) in your inbox by adding a mail filter. Most security software (see page 12) includes a mail filter.

- Most email packages, including free email accounts from providers such as Yahoo! Mail, Hotmail or Gmail, have spam filters built in.

what next?

See our free information guide *Avoiding scams* for more information on how to avoid email scams.

Telephone scams

Beware of a new type of telephone scam. The scammers call you claiming to be from the helpdesk of a well-known IT firm, such as Microsoft. They will tell you that your computer has a virus and will charge you to upload ‘anti-virus software’ for your computer. This turns out to be spyware, which is used to get hold of your personal details. Never respond to an unsolicited 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 don’t contact customers in this way.

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

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 using the internet is quick, convenient and can give you some great savings.

However, if you make purchases or do your banking online, you need to make sure that you protect your financial information. Use a secure website when entering credit card information. This means that the information you send cannot be read by anyone else. Some ways to spot a secure website are listed below.

- Look for a padlock symbol in the browser window. Don't be fooled by a padlock that appears on the web page itself.
- The website address should begin with 'https://'. The 's' stands for 'secure'.
- If you get a pop-up message warning you about a website's security certificate, be very cautious indeed. You may be redirected to a fake website, designed to get you to hand over your security details.
- 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 is not an absolute guarantee of safety.
- If the address bar is green, this is an additional sign that you're using a safe website.

Try these tips for shopping and banking online safely.

- Use a strong password that cannot be easily guessed by others. Avoid obvious ones like your mother's maiden name and opt for a random mix of upper and lower-case letters, numbers and keyboard symbols. For example, instead of 'football', use 'f00Tba1!'.
- If a deal looks too good to be true, it probably is. Cross-check information on the internet to see whether anyone else has had problems.
- Be extremely wary of anything that is offered in an unsolicited email.
- Use one credit card for internet transactions only. If anything goes wrong, you can always cancel this card.
- Never give out your financial details online unless you have complete confidence in the company. These companies will always give a full contact address and telephone number on the website.
- Use online retailers that have a good reputation, either as high-street shops or established online stores.
- Establish where the seller is based so that you can find out what consumer rights apply, as they vary from country to country. To find more information about buying from sellers based in other EU countries, you can visit the website of the UK European Consumer Centre (see page 18).

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, look at photos, find out about events and much more.

Friends Reunited (www.friendsreunited.co.uk) can help you find people you knew at school, work or in the armed forces. Websites such as Facebook (www.facebook.com) and Twitter (www.twitter.com) are a way to keep in touch with your friends and make new ones.

However, social networking sites can be targets for people who want to steal personal information. They are able to abuse the nature of these sites and gather personal details about its users through the information that users make publicly available about themselves.

Avoid these risks 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. Make sure that you read the terms and conditions of the site and that you only share information you are comfortable sharing.

- 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 (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 4).

what next?

For more information on social networking, see our free guide *Making the most of the internet*.

Protect your computer

Protecting your computer is simple. Follow the steps below to keep yourself secure. Start by doing a 'SAFE' check.

S = Spyware

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.

A = Anti-virus

Install **anti-virus** software. Without it you are at risk from viruses, which spread from computer to computer in email attachments and files downloaded from websites. If your computer is infected by one, it can make it slow or even leave you open to identity theft.

F = Firewall

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, so make sure that it's switched on.

There are many different types of anti-spyware, anti-virus and firewall software available. However, the best option for beginners is to purchase a suite of software from a reputable provider that includes all of these elements (see page 12). You can download these programs from the internet or visit a computer store on the high street to ask for guidance.

E = Ensure that your operating system is updated

The **operating system** – the main software programme on your computer – manages all the other programmes on it. The mostly widely used ones are Microsoft Windows and Mac OS. Generally, the latest version of an operating system is more secure than previous versions. For example, Windows 7 (released in 2009) is more secure than Windows Vista (released in 2007).

Whichever operating system you have, keep it updated as this will give you stronger protection. If you use Windows, find the Windows Update icon – this could be in your start menu or listed in 'All Programs', or 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.

If you have a wireless **router**, you also need to protect your **wireless network** so that people living nearby can't access it. A wireless router lets you access **broadband** internet from anywhere in your home. Read the instructions that come with your router to find out about how to set up defences. You will be able to use a 'key' – a type of password – so that no one else can access the internet through your router.

You should also get security software, such as Norton, McAfee or an effective free alternative such as Microsoft Security Essentials (if you have Windows 7 or Vista), AVG (http://free.avg.com) or Avast (www.avast.com/free-antivirus-download). This will protect your computer from viruses and spyware.

Once your software is installed, keep it up to date when prompted – this happens automatically (you just have to click ‘yes’ or ‘allow’ when asked). Online threats evolve constantly so this ensures that you have the highest level of protection.

You can find step-by-step explanations and advice on all of the above at www.getsafeonline.org. Microsoft’s Safety and Security Centre also has information on protecting yourself from scams. Visit www.microsoft.com/security/default.aspx

Whichever operating system you have, keep it updated as this will give you stronger protection.

Glossary

Anti-virus

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

Bandwidth

The speed of the connection to the internet. The higher the bandwidth, the faster it is to download something.

Broadband

A connection to the internet with high bandwidth. It is much faster than a dial-up connection, and is normally connected to the internet permanently. It does not tie up your telephone line. Examples of broadband connections include: ADSL, cable modem and fibre-optic leased lines.

Firewall

Firewalls prevent unauthorised access to your computer over the internet.

Internet Service Provider (ISP)

A company that provides access to the internet.

Modem

A device that links computers over the public telephone network, typically to connect to the internet.

Operating system

The software that manages different programs on a computer.

Phishing

An attempt at identity theft in which criminals lead users to a counterfeit website in the hope that they will disclose private information, such as usernames or passwords.

Router

A device that connects one or more computers to a broadband-enabled telephone line.

Social networking website

An online community where you can connect with 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 your computer slow and unreliable, or even make you a target for online criminals.

Wireless network

A way for your computer to connect to the internet without using wires/cables.

Useful organisations

Age UK

Age UK provides 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 169 65 65
www.agecymru.org.uk

In Northern Ireland, contact
Age NI: 0808 808 7575
www.ageni.org

In Scotland, contact
Age Scotland: 0845 125 9732
www.agescotland.org.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: 0845 404 0506 or 0845 404 0505
for a Welsh-speaking adviser
www.adviceguide.org.uk

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

Communities 2.0

A Welsh Government digital inclusion project. Offers support and advice to help communities do more online. Search its website to find local computer courses in Wales.

Tel: 0845 474 8282
www.communities2point0.org.uk

Digital Unite

Helps older people learn about computers and the internet. It has a network of tutors across Great Britain 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

Go on

Offers step-by-step information about how to use the internet safely and how to set up an email account. Use the site to find local computer courses.

www.go-on.co.uk

Gov.uk

Government website offering practical information and advice to the public.

www.gov.uk

Microsoft Safety and Security Centre

Offers tips on protecting your computer.

www.microsoft.com/security/default.aspx

UK European Consumer Centre

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

The Trading Standards Institute
1 Sylvan Court
Sylvan Way
Southfields Business Park
Basildon
Essex SS15 6TH

Tel: 0845 604 0503
Email: ecc@tsi.org.uk
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 77 1234
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: RSXZ-KTTS-KSHT, 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
Improving later life

We will use the information you have supplied to communicate with you according to data protection guidelines. Age UK (registered charity number 1128267) comprises the charity, its group of companies and national partners (Age Cymru, Age Scotland and Age NI). If you would prefer not to hear from them or carefully selected third parties, let us know by phoning 0800 107 8977.

Work & learning

You may be interested in other guides in this range

- *Making the most of the internet*
- *Working past retirement*
- *Your rights at work*

To order any of our **free** publications, please call Age UK Advice free on:

0800 169 65 65

www.ageuk.org.uk/workandlearning

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*
- *Leisure and learning*
- *Making the most of the internet*

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**.

Age UK is a charitable company limited by guarantee and registered in England and Wales (registered charity number 1128267
and registered company number 6825798). The registered address is Tavis House, 1–6 Tavistock Square, London WC1H 9NA.
Age UK and its subsidiary companies and charities form the Age UK Group, dedicated to improving later life. ID201100 02/13