TECHSENIOR
TECHNOLOGY FOR ASSISTING SENIORS

INTERNET SECURITY

STAYING SAFE ONLINE

Bath & North East Somerset ageUK

Internet security – staying safe online

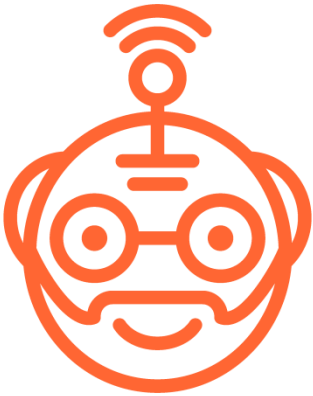
This guide provides general advice for people using the internet. It is intended to make you aware of the various things you can do to ensure you stay safe online.

The internet is a very useful tool to help you remain in touch with friends, shop, bank and find out about new hobbies and interests.

The internet has made life easier and is an excellent source of information, but it's important to use it safely and protect any device connecting to it.

You may not realise it, but you already have a lot of the skills and intuition to stay safe online. Just 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 and taking steps to avoid them means you can enjoy the internet safely.

TECHSenior, a project supported by the Erasmus+ Programme of the European Union, has created some online computer and internet training. This may be available near you, visit the website



www.techsenior.eu

Some words may not be familiar:

- **Virus protection** – this is a computer program which should be installed on your device to protect you (and updated daily – this usually happens automatically)
- **Searching the internet** for information (usually using a program called Google. In fact, 'to google' has become a verb (you may hear people talking about googling)

- You also search the internet for *websites* – these are 'addresses' that take you to the place you want to go. An example could be www.mybank.com, or www.bbc.co.uk
- **Emails** – people have their own email account (the equivalent of their own letterbox). You open an email account, get emails from friends, family and suppliers and you also send emails (sometimes with something attached, like a document or a photo – this is called an *'attachment'*)
- **Browser** – if you use chrome to search, this is your '*browser*'
- **Webpage** – this is the actual screen of the website you are visiting on the internet

Fear of the computer

A significant and frequently-voiced concern from many people is that mistakes made inadvertently could have serious consequences, such as sharing personal information, such as banking account details. But if you are aware and act sensibly, there is nothing to fear

Using the internet for banking or buying things

The internet can offer useful ways to do your shopping and manage your money from home.

It's quick and convenient and can even lead to some savings.

Booking holidays is another great use of the internet – you can see pictures of the hotel, read reviews from other people who have visited, or even use 'streetview' on Google maps to see what the area looks like.

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.

There are ways to ensure you are as secure as possible:

- Virus protection (see page 8)
- If buying something, 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.

- Many banks offer free anti-virus software or browser security products – check if your bank offers this.

- If a message suddenly pops up on the screen (often in a box) 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.

- 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.

- Always use a good strong password (see page 18) – this is good practice. You may need to keep a small notebook with your

passwords in – keep the notebook very safe.

One additional security measure could be to open a PayPal account. PayPal only exists to make secure payments and should therefore keep your bank/card details safe, then you don't have to give them to other sites/sellers

"If there are any attachments in it then I don't open them and delete the email" (Lynda aged 74).

But you might be missing something important. If you know who the email is from, there is nothing to fear

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.

Be positive

The internet can be a wonderful trigger for education and entertainment.
If you stay as safe as you can and report any worrying developments on your screen, then it should be a fun tool for you and your family.

Virus protection (software)

This is often in the news – a company or organisation has been 'hit' by a virus and cannot function properly.

And it's true – it does happen. But it happens less if you install anti-virus software (a program) and you get it updated daily. You can get anti-virus software free or you can pay an annual fee (in 2018, about £50 or 70 euros).

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

Another word to learn – '*malware*' – it simply means anything that is on your computer that you don't want – keep reading and you will come across '*spyware*' as well

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.

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.

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 same applies to the *operating system* 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.

Beginners and inexperienced IT users have a lack of confidence in installing updating software for fear of doing something wrong.

Understanding licensing agreements is sometimes at the root of this problem, as many do not understand the need to click 'yes' to install the software.

Don't forget your mobile phone or tablet (*such as iPad)*

These are also subject to viruses and other problems – same rules apply.

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

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 programs.

You should *'download'* these ONLY from reputable websites as you need to be wary, a download can be a source of viruses that you have invited onto your PC or other device.

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 applications are:

- Avast mobile security (visit www.avast.com)
- Norton mobile security (visit uk.norton.com/norton-mobile-security)

These apps work on phones and tablets that use Windows, Android and Apple products. They also work on PCs and laptops.

It is possible to purchase a licence to cover all your technical devices; that's a much easier option.

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.

"When I first started, a message used to come up, saying 'you have just done an illegal entry and the computer needs to close down'. I shut the windows because I thought the police were coming". It took me a while to realise it was a computer message !!

(Molly aged 67)

Emails – a great way to be connected

New words to learn – *spam* and *phishing*

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 (they may go directly to your 'junk mail' folder). However, it's still important to be aware of the common types of email scams so that you can protect your personal information – some do get through to your 'INBOX'.

It's great to keep in touch with family and friends who live in different countries – so much quicker than a letter – and you don't need to buy stamps

Spam, or junk mail, is usually from a person or organisation trying to sell something – just as it comes through your own letterbox.

Most email providers (such as Gmail. Yahoo Mail or Hotmail) have spam filters or anti-spam protection to automatically block emails from untrustworthy sources. Sometimes a legitimate email gets accidentally into your 'junk mail'.

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 – and suggests you click onto their website
- an email encouraging you to send the email onto more people.

Sometimes accounts can be hacked into and fake emails sent out to all of that person's contacts; so it could

come from a known friend or family member.

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 in UK) 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.

• 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.

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.

"My granddaughter has just got a job working on a ship cruising the Caribbean and if I don't hear from her for a few days I start worrying, because she has never left home. I send her an email and say answer me straight away and next day I have a reply. It's fantastic" (June aged 76).

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.

Be aware of calls from your bank or police about fraudulent use of your credit or debit card – they will not do that – so hang up.

A scammer will ask for your PIN number and may tell you to give your bank card to a courier that they will send to your home. This is a common scam and your bank would never do this.

If a caller asks you for personal information such as your PIN number, says they will send a courier to collect your card, or tells you your computer has a virus, ignore what they are saying and hang up. These are common scams.

Be aware that scammers can keep your phone line open. Scammers may ask you to call an official number, such as the one on your bank card. They can keep the phone line open so even if you hang up and dial the

bank's number, the line is still connected to the scammers. Always use a different phone, call someone you know first to check the line is free, or wait at least 10 to 15 minutes between calls to make sure any scammers have hung up.

Email and online scams are very common. Scammer's techniques also change frequently as they develop new ways to defraud people.

Like scams using postal mails, or people knocking on your door, use common sense and take your time to assess is it real – or is it a SCAM

"You read about scams in the paper and it makes me think how can you recognise a scam website?" (Mark aged 69).

If you have been reading – you know the answer

But just think of the benefits and what you can do using the internet for research and finding out things – even as simple as 'what's on' locally

"My favourite occupation is producing my Family Tree....It has become the most compelling thing I've undertaken with IT technologies; finding sites of place names, their origins and looking for yet more leads to family" (Mike aged 59).

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

- password
- 123456
- password123

Don't use your date of birth, house number or a name that can easily be guessed.

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 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

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 others.

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. Don't use the password manager on a public computer, for example in a library – to prevent strangers accessing your account.

"Okay your father managed to get a mouse. Now how do we use it?"

"I was dragged kicking and screaming into the twenty-first century.

I was very reluctant because I am petrified of new technology.

But with a lot of persuasion, primarily from my GP who thought I would enjoy it, it would stimulate me, I eventually bought one" (Mary aged 61).

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.

- Although it's nice to share your holiday photos with family and friends – this is not a good idea as it advertises to anyone that you are away. Share them when you return home.
- Use a strong password that is different from the passwords you use for other accounts
- 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

Ever heard of skype?

This is a great way to keep in touch with friends and family, ever across the other side of the world. And if you have wifi – the news is even better – you can talk for free.

You can do the same with WhatsApp – download this to your tablet or smartphone – talk for hours to your family in Australia, Malaysia or even just across Europe. And it doesn't cost you money.

IT IS EASY TO STAY SAFE

JUST BE AWARE

AND BE SENSIBLE

NOTES:

This document reflects the views only of the authors and the Commission cannot be held responsible for any use which may be made of the information contained therein. Supported by the Erasmus+ Programme of the European Union