



# Using the internet safely














# Contents

|   |    |
|---|----|
| Introduction - Reasons for using the internet | 03 |
| How to protect my personal data               | 04 |
| Public and private space                      | 08 |
| Making friends on the internet                | 10 |
| How to stay safe on social media              | 14 |
| Harassment on the internet                    | 18 |
| Browsing the internet safely                  | 22 |
| Phishing emails                               | 26 |
| Conclusion                                    | 30 |

# Introduction

**The internet is very important in our lives.**

We can use the internet to:

-  • talk with friends and family (for example, with WhatsApp and Messenger)
-  • work and talk with colleagues and clients
-  • email people and organisations
-  • look for jobs
-  • shop (for example on Amazon and other online stores)
-  • look for information (for example, on Google or Wikipedia)
-  • find directions and use maps (for example, on Google Maps)
-  • learn about new things ('How to' videos and online courses)
-  • book holidays and train journeys
-  • use social media (for example, Facebook and Instagram)
-  • read and watch the news
-  • listen to music, watch films and television (such as IPlayer, Netflix, Youtube, Spotify) or play video games
-  • meet new people

You need to be confident about using the internet. It is important for lots of jobs.












This guide will give you tips and advice on how to use it safely.



The internet and social media are great for sharing news with your friends and family. However, you must know what personal information you can share and what information you must keep private. This is important because it will help you to keep safe.




### What is personal data?

Personal data is information about you which helps people identify who you are. For example:

- |   |   |  |
|---|---|--|
|  name                    |  telephone numbers                 |  information about your health                 |
|  passport details        |  date of birth                     |  friends and family                            |
|  passwords and pin codes |  finance, bank and payment details |  photos and videos                             |
|  email address           |  places you visit or holidays      |  your gender, sexuality, and ethnic background |
|  postal address          |  details about your job            |  |

### When do you need to share personal data?










Here are some examples:

-  When you shop online, they often ask you for your name and address. This is to check they match your payment details.
-  When you register to use social media or an online game, you provide your name and date of birth to show you are not a child. You may also be asked some security questions, in case you forget your password. For example: the name of your first pet or your first school.
-  When you visit government websites, they may ask for your name and address to check you match their records and that you are the right person.



However, please remember that everything you share on the internet can stay there forever!

### If strangers access your personal data, they could:

-  • connect to your social media accounts or websites and steal your personal information
-  • contact your friends, family and people where you work
-  • steal your money
-  • steal your identity and pretend they are you
-  • share your private photos and embarrass you
-  • bully or hurt you
-  • stalk you (this means following what you do without you knowing it)
-  • know when you are on holiday and burgle your house
-  • send you unwanted emails and adverts

But there are lots of things you can do to stop this happening and keep your personal data safe:



**Do not publish your personal information online** or keep it to a minimum



**Think about who can see your photos and information** before you publish them



If you want to publish pictures of your friends, **ask for their permission first**



**Keep your social media private** and do not accept 'friends' you do not know



**Always log out** from your accounts, especially if other people use the same computer



**Do not give out your personal information**, if someone asks for it



**Do not publish your full name.** Only use your first name or a nickname



**Never share your passwords**



**How to protect your personal data?**



**Never share your bank details**



**Never share your address or phone numbers**



There are public and private spaces on the internet. It is important to understand the difference because private spaces are safer.

### What is the difference between a public and a private space?



**A public space is like a park.** You cannot be alone and you cannot control who is coming in. People you don't know can come in without your permission and everyone can see what you do and hear what you say. You are not in control of the information you publish in a public space.



**A private space is like a room.** It is a place where you can be alone. Only the people you decide to invite in can see what you do and hear what you say. You are in control of the information you publish in a private space. Only invite people you trust into private spaces because they could share your information outside the room.



The internet and social media are public spaces. Everyone can see the information or the pictures and videos you publish, without your permission.



Try to google your name and see all the information strangers can find out about you easily.

### Why is it not safe to publish information in a public space?



- People you don't know could access your information and use it to hurt you



- Criminals could see if someone is on holiday and know when to burgle their empty home



- Your boss, your parents or customers could find out what you do in your private life



But there are some private spaces on the internet. For example, only you can see the information you share on government websites or NHS websites.



You can make your social media account private so only the people you accept as friends (on Facebook) or followers (on Twitter and Instagram) can see your posts and pictures.



On Facebook, you can choose who sees your information. For example, you may not want your parents to see pictures of you with your friends.

### Tips:



- Make sure your social media accounts are private



- Think before publishing information about yourself



- Do not publish personal information in a public space



The internet is a great way to keep contact with friends and family and to connect with people from all around the world. On the internet you can talk to:



friends



shops and customer services



family



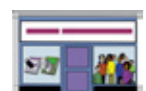
celebrities and influencers



colleagues



people you've never met before



organisations

### But there are some risks in talking to people you don't know on the internet:



People could use a fake name, fake pictures and a fake age. ('Fake' means something that isn't true)



People could try to be your friend in order to get your help, ask for money or steal your information



When you accept a stranger's invitation to be your friend online, you give them access to your private information

### Who you should not accept as a friend:



- In general do not accept people you don't know



- People you know in real life that are not nice to you



- Your boss and other people you work with, as you may not want them to know about your private life



- People who have no clear photos or who use photos of famous people



- People you do not have any friends in common with

### Be careful if someone you don't know:



- messages you



- asks for help or money



- asks you lots of personal information (your date of birth, home address, work or school) or asks you for your pictures



- asks to meet you in a private place



- asks to become your girlfriend or boyfriend



- is being too nice

If the person doesn't know you, this is not normal behaviour



**Remember that a stranger can be a risk**



On social media you should **only accept people you know** as friends or followers



**Ask your friends** if they know this person



If you have any questions or doubts, **ask someone you trust to give you advice**



**Do not make friends quickly** with someone you meet online. Take time to get to know them before you share any personal details about your life



**Do not share personal information** such as your address or passwords



**Trust your instincts.** If you feel unsafe, stay away and speak to someone you trust








**Do not send personal or naked pictures** of yourself to anyone



**Usually you should not meet someone you have met on the internet.** If you really want to meet the person, speak first to someone you trust. Only meet them in a public space. Never get into their car. Ask a friend or family to go with you the first time.

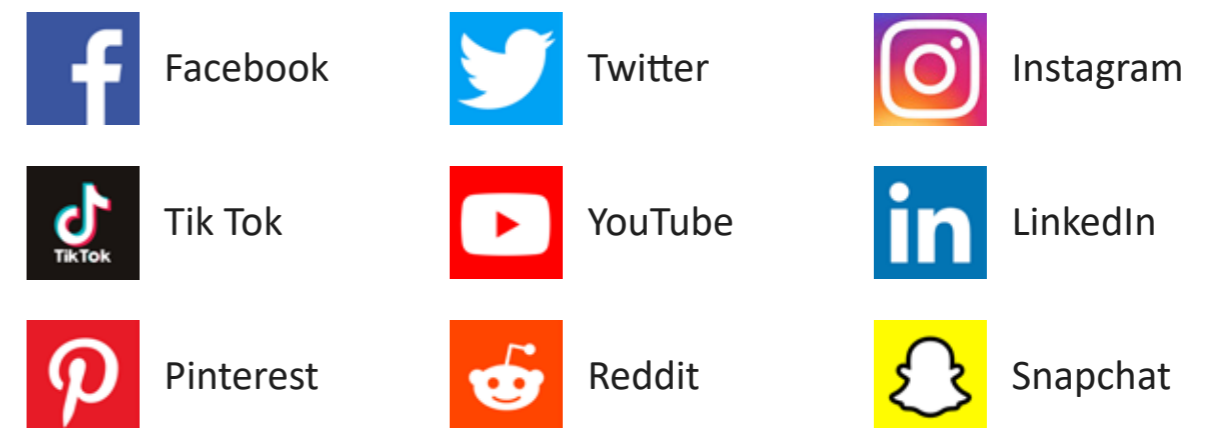


### Social media can be great and fun. On social media you can:

-  • express yourself
-  • share pictures of your activities
-  • connect with friends and family
-  • connect with people around the world, including famous people
-  • get information about your friends' activities and see their pictures




### There are many different social media platforms.

For example:



### But there are some risks on social media.

Here are some examples of risks on social media:

-  Someone could pretend to be someone else. If you accept their friend request, they could steal your private information
-  Some people could invite you to click on a link so that they can steal your information or infect your computer with a virus
-  Some people could also spread some bad information or embarrassing pictures about you on the internet

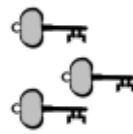




Keep your social media accounts private: only people you accept as friends can see your information



Do not accept friend requests from people you don't know



Use different passwords for all your social media accounts



Don't publish too many details about your life



Do not publish pictures that you don't want your family or people you work with to see



Spam emails or junk emails are unwanted messages. They may ask you for money or ask you to click on links. Do not open them - just delete them!



## How to stay safe on social media



Never use social media to send private pictures. You will have no control over what people do with them



Remember that you can change who can see your pictures and posts on Facebook, and you can block friends



Do not respond to someone who is not being nice to you



Never publish your home address, email address, phone number or passwords








If you have any problems and don't know what to do, speak to someone you trust



One risk people can face online is harassment. It is important to know what it is and how to act.






### What is harassment?

Harassment is when people are being aggressive, being intimidating or putting pressure on you. Here are some examples:

-  **Bullying:** This is when you receive many bad and negative messages online from someone or a group of people or when people are sharing rumours on social media about you to make you feel bad and sad
-  **Discrimination:** This is when someone is treating you unfairly or unequally because of your ethnic background, your impairment, your gender, your sexuality or your religion
-  **Grooming:** This is when someone tries to become your friend to take your money or take advantage of you in some other way
-  **Sexting:** This is when people send sexual messages or naked pictures and videos, without your consent
-  **Stalking:** This is when someone is spying on you and trying to find out everything you do, without your consent

### Trust your instincts.

It is not always easy to know when we are being harassed. The best thing to do is to listen to your feelings. If you have the following feelings, this means that something is probably wrong and you should talk to someone:

-  • you feel sad
-  • you feel nervous
-  • you feel unhappy
-  • you feel angry
-  • you feel bad

## Here is what you need to do if you have a problem:



**1) Do not respond** and do not interact with these people



**2) Do not rush. Keep evidence** of the bad pictures or messages you receive so you can show them to someone you trust or to the police



**3) Disconnect** – log off from the internet and turn off your laptop or phone



**4) Talk to someone you trust** about what happened – ask your family, a friend or your college tutor to help you



**5) Block** – On Facebook, Twitter and Instagram you can block someone who treats you badly. When you block them they cannot message you or see your posts and information anymore



**6) Make a report to the social media company** – Most social media or dating apps have a report button. When you do this, the website may decide to block them for their bad behaviour



**7) Make a report to the police** – You should contact the police if someone has treated you very badly or stolen your money or private information. Deaf people or people who have difficulty with speech can download an app or use their textphones to contact emergency services. Go to Relay UK for more information: [www.relayuk.bt.com/how-to-use-relay-uk/contact-999-using-relay-uk.html](http://www.relayuk.bt.com/how-to-use-relay-uk/contact-999-using-relay-uk.html)

## Hate crime:

A hate crime is when somebody commits a crime against a person because of a reason that makes them seem different, such as their race or religion, or because they are Disabled. This includes **verbal abuse, online abuse, harassment or violence** from strangers, neighbours or people you know well.



These organisations can help you, if you think you have experienced a hate crime:

- **Disabled People's Organisations in London:**  
[www.inclusionlondon.org.uk/directory/services/disability-hate-crime-support/](http://www.inclusionlondon.org.uk/directory/services/disability-hate-crime-support/)
- **The Community Alliance to Combat Hate (CATCH)**  
[www.catch-hatecrime.org.uk](http://www.catch-hatecrime.org.uk)
- **Bullying UK**  
[www.bullying.co.uk/cyberbullying/](http://www.bullying.co.uk/cyberbullying/)  
Tel: 0808 800 2222
- **Hatecrime UK**  
[www.stophateuk.org/report-learning-disability-hate-crime/](http://www.stophateuk.org/report-learning-disability-hate-crime/)  
Tel: 0808 802 1155  
This service is not available in all London boroughs. Please check the list on the webpage

## Useful resources:

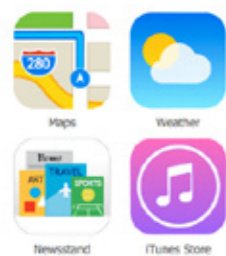
- [www.inclusionlondon.org.uk/campaigns-and-policy/facts-and-information/hate-crime/am-i-being-targeted-due-to-my-disability/](http://www.inclusionlondon.org.uk/campaigns-and-policy/facts-and-information/hate-crime/am-i-being-targeted-due-to-my-disability/)
- [www.report-it.org.uk/files/disability\\_hate\\_crime\\_book\\_low.pdf](http://www.report-it.org.uk/files/disability_hate_crime_book_low.pdf)



**There are different ways you can use the internet:**







**Via web browser software** such as Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome or Safari. We use web browsers mostly on laptops and computers to visit websites.







**Via mobile applications (or apps).** A mobile app is software used on mobile phones and tablets. Most websites and social media platforms also have a mobile app.

**There are a few risks when browsing the internet:**





-  • People can steal your personal information
-  • People can steal your payment details and use them to buy things without your agreement
-  • Social media and email accounts can be hacked
-  • You can get a virus on your computer

**You can avoid these risks by making your websites, social media and email accounts secure:**







-  • Use strong passwords. Never use easy passwords, such as “123456” or “123abc”. Avoid using your name, your birthday, or any other information that someone else may already know about you. Include numbers, lowercase and uppercase characters and special characters like “£%&”
-  • Change your passwords regularly
-  • Use different passwords for your accounts
-  • Never give your password to anyone
-  • Use Two-Factor Authentication whenever you can, for example on Facebook. As well as a password, you will also need to enter a special code (which is sent to your phone). This makes your accounts very safe.
-  • Do not give your mobile phone or tablet to someone
-  • Use a password on your laptop; and a pin code on your phone
-  • Always remember to log off when finished
-  • If there is any problem, it is better to change your password
-  • Keep all your accounts private

### Be extra careful if you use the internet in a public place.




Sometimes we use the internet on our friends' computers or in public places like libraries and community centers. We also use the internet on our phones in public spaces. Here are some tips on how to stay safe, if you use the internet in a public place:

-  • Make sure that nobody can see your screen and the personal information you are entering (passwords, payment details)
-  • Never save your password on a laptop/computer that is not your own
-  • Always remember to log off from all the websites (emails and bank accounts) or social media you visit
-  • Always remember to turn off your phone, if you leave it somewhere

### Tips on how to surf the internet safely on a web browser:






-  • Only visit trusted websites. Make sure the website address starts with "https" - this means it is safe. Never enter your personal details into a website that starts "http", with no "s"
-  • Be careful with public WIFI connections, as hackers could position themselves between you and the connection point
-  • Don't click on links from a website you don't know
-  • Install antivirus software to protect your computer or laptop against viruses
-  • It may be better to go online with someone you trust or tell them if you are unsure or feel unsafe
-  • Back up your files so you don't lose them. For example, use an external hard drive

### Paying on the internet.

-  • If you aren't used to paying for things on the internet, ask someone you really trust for support when you need to pay for something online
-  • Only make payments on trusted websites ("https://") and to companies you know
-  • Do not let anyone see your credit card and online payment details when you are in public

### What do I do if I get hacked?


Getting "hacked" means that someone has taken control of your website, one of your social media accounts or your email address and sent messages on your behalf to all your contacts.


-  **1) Change your password**
-  **2) If you have the same password on all your social media accounts, change it on every account.** Create a different password for each account
-  **3) Check your bank account.** If you find a payment that you didn't authorise, contact your bank immediately
-  **4) Check your 'Sent' box.** If emails have been sent to your contacts on your behalf, email or message all your contacts to tell them that your account has been hacked. Advise them not to respond to messages previously sent from your account
-  **5) Do a scan of your computer / laptop** with your antivirus software



On the internet, we send and receive a lot of emails, as well as messages (WhatsApp or Messenger). But occasionally we receive some emails that can put us at risk. It is important to spot those emails so that we stay safe.









### There are two different kinds of emails you need to be careful with:

 **Spam emails.** These are emails you receive from people and companies you do not know and that you have not given permission to contact you.

 **Phishing emails.** These emails look like genuine emails from companies. However, they are designed to get hold of your personal information, your money or pass on viruses. These are dangerous because they often look real and convincing. Sometimes they look like emails from companies you already deal with.

### How do I recognise a phishing email?

These emails:

-  • put you under pressure and ask you to act urgently. For example, they may say, “Action required”, “Click immediately” or “Your account will be blocked in 24 hours, if you don’t click on the link”
-  • ask for your credit card details, financial information or your passwords
-  • ask you to click on a link to make a payment or to sort out an error
-  • have a document attached
-  • have an email address which is different from the real company’s website address
-  • have a lot of grammar or spelling mistakes
-  • use a lot of technical words, to scare you
-  • offer you money or look too good to be true



**Take a moment to think** and ask yourself if it is a phishing / spam email or not



**Always look at the email address.** If the information after the “@” is different from the sender’s name or from the official web address of the company, it is a **fake email**. Also, do not trust the website if it starts with “http://”. It should be “https://”



**Mark the email as spam**, block the sender and delete the email. You can report bad messages to social media companies



**Be careful when you give your email address to websites or apps.** This could result in you getting spam and phishing emails



**Never respond** to phishing or spam emails



If you don’t recognise the sender, company or email address, **do not click on the link** or open the attachment



If you feel unsure or uncertain about something, **talk to someone you trust as soon as possible**



**Don’t share your personal information or send money** to anyone you don’t know

# Conclusion

Finally, here are 10 very important tips to keep you safe when you use the internet:

-  **1)** Follow your instinct: Always talk to someone you trust if you feel bad, sad or have any problems
-  **2)** Never share personal information such as your full name, address, date of birth, payment details or passwords
-  **3)** Think before publishing pictures or information about yourself. Remember that everything you publish on the internet can stay there forever and be seen by everyone
-  **4)** Use strong and different passwords for all your accounts
-  **5)** Keep your social media accounts and websites private
-  **6)** Only accept friend requests from people you know
-  **7)** Never interact with people who are bullying you. Report their behaviour and block them
-  **8)** Only visit and pay for things on trusted websites
-  **9)** Think before you click on links in emails, on websites and social media platforms
-  **10)** Do not save passwords on computers that do not belong to you and be careful when using the internet in public places

Remember! The internet is a great place to work, to have fun watching films and playing games, to study and find information, and to stay in touch with friends and family. Follow these tips and enjoy using the internet safely!

# My 10 top tips

After reading this guide, write down 10 things you will do to stay safe when you use the internet:

|                 |                  |
|-----------------|------------------|
| My tip number 1 | My tip number 2  |
| My tip number 3 | My tip number 4  |
| My tip number 5 | My tip number 6  |
| My tip number 7 | My tip number 8  |
| My tip number 9 | My tip number 10 |



Inclusion London promotes equality and inclusion for Deaf and Disabled people by supporting the development of Deaf and Disabled People's Organisations (DDPOs) across London. We run the 'Making it Work' programme which aims to improve young Disabled people's chances of finding employment and remove the barriers to getting into work.

*[www.inclusionlondon.org.uk](http://www.inclusionlondon.org.uk)*

**Produced by Inclusion London,  
August 2021**

**Copyright:** We welcome reproduction of any part of this resource but we request that Inclusion London is acknowledged. Inclusion London has endeavoured to ensure that information included in this resource is up to date and correct. However, this cannot be guaranteed and it is, therefore, the responsibility of readers to seek their own legal advice where necessary.

Design: Raphaël Harfaux