DU
Digital Unite

How to stay safe online

🖨 **Print this guide**

The World Wide Web is a fantastic resource, but as with everything, it has its risks. This guide will give you some hints and tips on staying safe while enjoying this new online world.

Follow these step-by-step instructions to help you stay safe online

This guide is written for Windows 10 computers.

General safety advice

Step 1: Make sure your antivirus software is up to date. If you're not sure whether you have antivirus, read our guides What is antivirus? and Antivirus: how to get virus protection.

Step 2: Check that the Windows firewall is switched on. To adjust your Windows firewall, go to control panel on your computer or type in Windows Firewall in the search bar.

This will bring up the Windows Firewall dialog where you can control all of the various settings for the firewall.

Step 3: If you have an earlier version of Windows, a red shield-like icon in the system tray will appear if the Windows firewall isn't switched on. Click it to see options for rectifying the problem.

Using the internet on shared computers

If you use the internet on a shared computer – for instance, in a library or internet café – try to remember to use the InPrivate Browsing option in Microsoft Edge. When you do, you don't leave any trace of the websites you've visited. Remember to log out of any email or social media accounts before you walk away from the computer.

Step 1: Click on your browsers settings and enable 'New InPrivate window'.

⬜ New window		Ctrl+N
▨ New InPrivate window		Ctrl+Shift+P
Zoom	— 100% + ⤢	
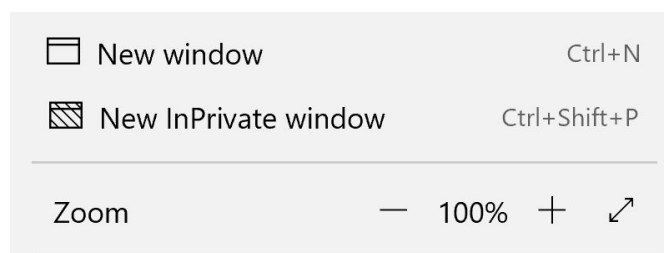
Step 2: The address bar will now look like this. This tells you that you can browse the internet in the normal way but without revealing your online 'journey' to anyone else.

| ▨ InPrivate | ⬜ InPrivate | ✕ | + |
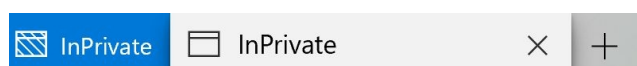
Step 3: To switch off InPrivate Browsing, just close the browser window.

Step 4: If you forget to use InPrivate Browsing, you can still get rid of the details of what you looked at. For more information, see our guide How to delete internet history.

To keep your browser secure, we recommend that you clear your browsing history, cache and cookies regularly.

Cookies are small pieces of data from a website and stored in your browser while you're on a website. Every time you pull up that same website, the browser sends the cookie back to the website with all the info from the last visit. Sometimes, the cookies are used to track your visit to websites so that businesses can show you ads online.

Other good things to do

- If you use wireless broadband, make sure it's password-protected to prevent other people from using it or hacking into it.

- Keep your passwords secret and don't use the same one for everything. Read our guide How to choose a password. We recommend that you update your password regularly.

- Email attachments can contain viruses so never open them unless you're confident that they're from a reliable source. If an email looks suspicious, it's best to delete it or report it to Spam.

- Beware of 'phishing' emails, these often look like they've come from a bank or similar institution and usually ask you to click a link to verify your identity. These emails are never genuine and should always be deleted.

- When shopping online, only use reputable sites. The Shopsafe website has a directory of secure UK shops as well as advice on safe online shopping. Never submit any personal information if you are unsure.

- Before entering any personal or payment information online, always check that you're on a secure website. This is indicated by a yellow padlock icon at the top of the screen and a website address that starts with 'https://' (the 's' stands for 'secure').

- Use a nickname rather than your real name when participating in online chatrooms or forums and don't give out any personal information.

- If you use social networking sites – for instance, Facebook – change your account security settings to limit who can see your profile information. Never update your status with information that you wouldn't want to be made public.

- If you are applying for jobs online make sure your CV does not contain any personal information like your home address.

- For further advice on staying safe online, have a look at the Get Safe Online website.

Last updated on January 2023

Next steps

▶ Email safety tips

▶ Keeping your children safe online

▶ How to stay safe online

▶ How to shop safely online

▶ What is identity theft?

▶ How to protect yourself from identity theft

▶ How to delete internet browsing history

▶ How to delete Favourites

▶ What is Antivirus?

▶ Antivirus: how to get virus protection

▶ How to choose a strong password

How do digital skills change lives?

Find out about Digital Inclusion

DU
Digital Unite

📞 0800 228 9272

💬 du@digitalunite.com

Get in touch

Privacy policy

Terms of use

Cookie policy

Our learning platforms

Digital Champions Network

Inspire
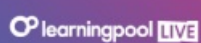
Our newsletter

Research, resources, insights and offers.