Skip to main content

How to shop safely online

Print this guide

Using the internet to buy items or services can save a lot of time and effort, you can sit in the comfort of your home and browse without using shoe leather. However, there are unfortunately some risks when online shopping including fraud if you've made payments over unsecured web pages, bogus online shops or buying fake good. It's important to know who you are buying from, how much you are paying and that your purchase is secure and safe. Here are our top tips for shopping safely online:

1. Ensure the store is legitimate

Does the online shop have a telephone number and contact details so if you have any problems you can contact someone directly? Check particularly for a physical address, if it doesn't have one then it could be risky. If you haven't heard of the shop before, check out any reviews or do a search online to establish whether they are genuine or not. There are also sites you can consult such as Shopsafe, which has checked out more than 4,000 shops and rated them for their range of goods, delivery costs and security.

2. Pay by credit card

If you pay by credit card rather than a banking debit card, this gives more protection should there be any problems with your purchase, your card is used fraudulently or you don't get your goods.

3. Be vigilant

Check, check and check again your purchase before paying. Is it exactly what you want, does the price include VAT and is there any extra delivery to pay.

When you get to payment check that the page is secure before you give any details of cards etc. If it is a secure page it will show a padlock in the address bar at the top of the screen. Also, it will have an address starting with https:// to show that it is secure. The address bar will also go green if the website is secure (this can only be seen however if you are using the latest updated version of your browser, so always check you have the latest version to be up to date with security features).

4. Keep your bank details safe

Never make payments directly to an individual's bank account – always use a secure payment method such as PayPal, which never discloses your banking details to the other party.

5. Always log out of sites if you have registered your details or logged in

Just closing the window will not remove your details and someone coming after you, particularly in a public place may still be able to see your personal details if they open up the internet browser again. If you have registered your details and use a password, try to use different passwords and make the password difficult to guess with numbers and letters.

6. Get protection

Always ensure that you have antivirus or malware software installed and a firewall to stop any unwanted attention from hackers or viruses that can access your personal information or take you to websites that aren’t legitimate. Always double check the website address before you submit any details and look for any irregularities. If it looks odd or isn't the address you'd expect it to be, don't enter any personal information.

Remember to update your browser as new versions have added security benefits. updates will keep you ahead of identity thieves and keep your private information safe.

7. Check your statements

After any transaction check your credit card and bank statements to ensure that the correct amount was taken from your account and inform your bank or credit card provider immediately if you have any concerns.

8. Public Wi-Fi

Free public Wi-Fi can easily be intercepted so it is always a good idea to take caution when logging into public Wi-Fi networks through your phone or tablet device. Treat all Wi-Fi links with suspicion and don't assume that all Wi-Fi networks are legitimate. Check that the Wi-Fi access point is genuine by looking closely at the Wi-Fi name.

Use a VPN (virtual private network) to connect to a public Wi-Fi network, this will encrypt all your data that passes through the network. Also, avoid logging into websites that capture personal information such as bank account details and any websites that store credit card information.

9. Update your passwords

Changing your passwords regularly on all of your online accounts is important to keep your accounts secure. We highly recommend not using the same password across all of your accounts to avoid them being compromised.

10. Being aware of emails

Do not click on links in suspicious emails. Many phishing scams involve emails from what seems like legitimate sites. If you come across an email like this do not provide any financial or personal information to them. If you have any doubts, search for the company's website, or contact them.

11. Read the company's policy

Reading the company's privacy policy is the only way to know for sure what a company does with a user' information. It is important to check in their policy that your personal data isn't being sold to third-parties and that it is encrypted and secure.

Here are some articles that we recommend:

- Safer online shopping
- Smartphone security
- Protecting your money online

Last updated February 2023

Next steps

- Internet shopping: how to buy online
- How to stay safe online
- Email safety tips
- Keeping your children safe online
- Staying safe playing online bingo

How do digital skills change lives?

Find out about Digital Inclusion