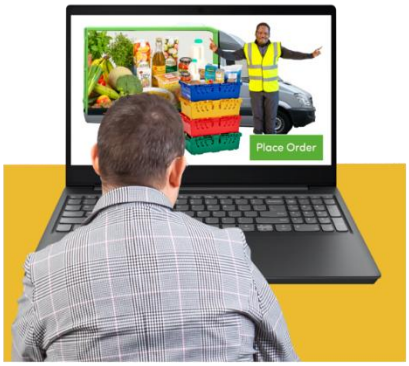
Shopping online safely



Choose carefully where you shop

If you are shopping online get some information about the business you want to buy from.

Read feedback from people or organisations that you trust on consumer websites like Which? or Trustpilot.

Some of the emails or texts you get about amazing offers may have links to **fake** websites.

Fake means it is not real.

If you are not sure if the link is real, do not click on it.

Instead:

- type a website address that you trust directly into the address bar at the top of your computer screen
- or search for the website and follow the search results

Use a credit card for paying for things online

If you have a credit card, use it when you shop online.

Most major credit card companies protect online purchases.

In most cases they will **refund** you – give you your money back – if things go wrong.

Using a credit card rather than a debit card also means that if your payment details are stolen, your main bank account will not be affected.

If you are using a credit card, remember to pay back the **balance.**

The **balance** is the amount of money you need to pay back.

If you do not pay back the balance it will cost you more in **charges** and **interest** – costs for borrowing money.

Debit card payments and purchases are not covered by the law called the Consumer Credit Act.

You might be able to make a claim for a refund using a scheme called ‘chargeback’.

An **online payment platform** is a service that links your payment with the organisation you are buying from.

Think about using an **online payment platform** like PayPal, Apple Pay or Google Pay.

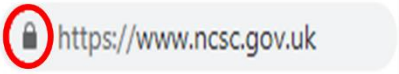
Using one of these ways means the organisation you are buying from does not see your payment information.

They also have their own ways of sorting problems if anything goes wrong.

They may not provide the same protection as a card provider.

Check their **terms and conditions** before you sign up to use them.

Terms and conditions are the rights and responsibilities that you and the seller agree to.



When it is time to pay for your items, check there's a 'closed padlock' image in the browser's address bar at the top of your screen.

It means that the connection is secure.

It will look like this picture on the left.

The padlock icon does not mean that the organisation you are buying from is real or honest or that their website is secure.

You should still be careful.

If the padlock icon is not there, or the browser says not secure, then do not use the site.

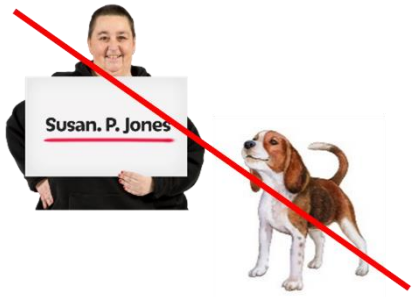
Do not enter any personal or payment details or make an account.

Only give the details you need to

When you are buying something online, only fill out the details you have to.

These are usually marked with an asterisk, and will usually include your delivery address and payment details.

An asterisk looks like this: *



Do not give them information like your mother's maiden name, or the name of your first pet if you are asked to do this to complete your purchase.

You may be asked if you want to:

- make an account for an online store
- save your payment details to make it quicker next time you shop with them

Do not allow this if you are only using the online shop once.

If you do not get the item you bought online, or it does not match the description given, Citizens Advice has some useful information about getting your money back if you paid by credit card, debit card or PayPal.

Keep your accounts safe and secure

- do not use the same password for all your online accounts
- do not use passwords that could be easily guessed

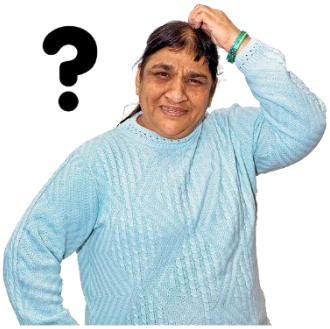
Online criminals could guess your password and use it to get into your other accounts.

Make sure that your important accounts are protected by strong passwords that you do not use anywhere else.

Important accounts are your:

- email account
- social media accounts
- banking accounts
- shopping accounts
- and payment accounts like PayPal

Having strong passwords for all your online accounts and remembering them is hard.



Check this information about making strong passwords from three random words like ‘applefishpen’.

It also explains how to store passwords safely, so you do not need to remember them.

You can protect your important accounts by turning on 2-step verification (2SV).

It stops online criminals from getting into your accounts, even if they know your password.

It asks you to confirm that it is really you by getting you to enter a code that is sent to your phone.

Suspicious emails, text messages and websites

If something looks **suspicious** it means you do not trust it because it does not look right.

Fake emails can be very difficult to spot.

Fake emails sometimes have links designed to steal your money and personal details.

Do not panic if you have replied to a suspicious email or text message or visited a scam website.

If something does not feel right, follow this guidance on dealing with suspicious emails and text messages.

If you get an email which you are not sure about, forward it to the Suspicious Email Reporting Service (SERS) at report@phishing.gov.uk

If you get a text message you are not sure about, forward it to 7726.

It is free to do this.

If you have visited a website you think is trying to scam you, report it to the NCSC using their online form.

If you see an advert online that you think might be a scam, report it using the online form on the Advertising Standards Authority (ASA) website.

ASA can ask organisations to take information off their websites.

If things go wrong

If you think your credit or debit card has been used by someone else, let your bank know straight away so they can block anyone using it.

Always contact your bank using the official website or phone number.

Do not use the links or contact details in a message you have been sent or given over the phone.

If you have lost money, tell your bank and report it as a crime to Police Scotland:

- by phoning 101
- by using their online Contact Us form

- in person – find your local Police Stations and check the Public Counter opening hours

- by using Text Relay - 18001101 for people who are deaf, deafened, or who find it difficult to talk

People who use British Sign Language can use the Contact Scotland service.

If you tell the police about a scam, you are helping to stop other people being scammed.

 Prepared by Disability Equality Scotland