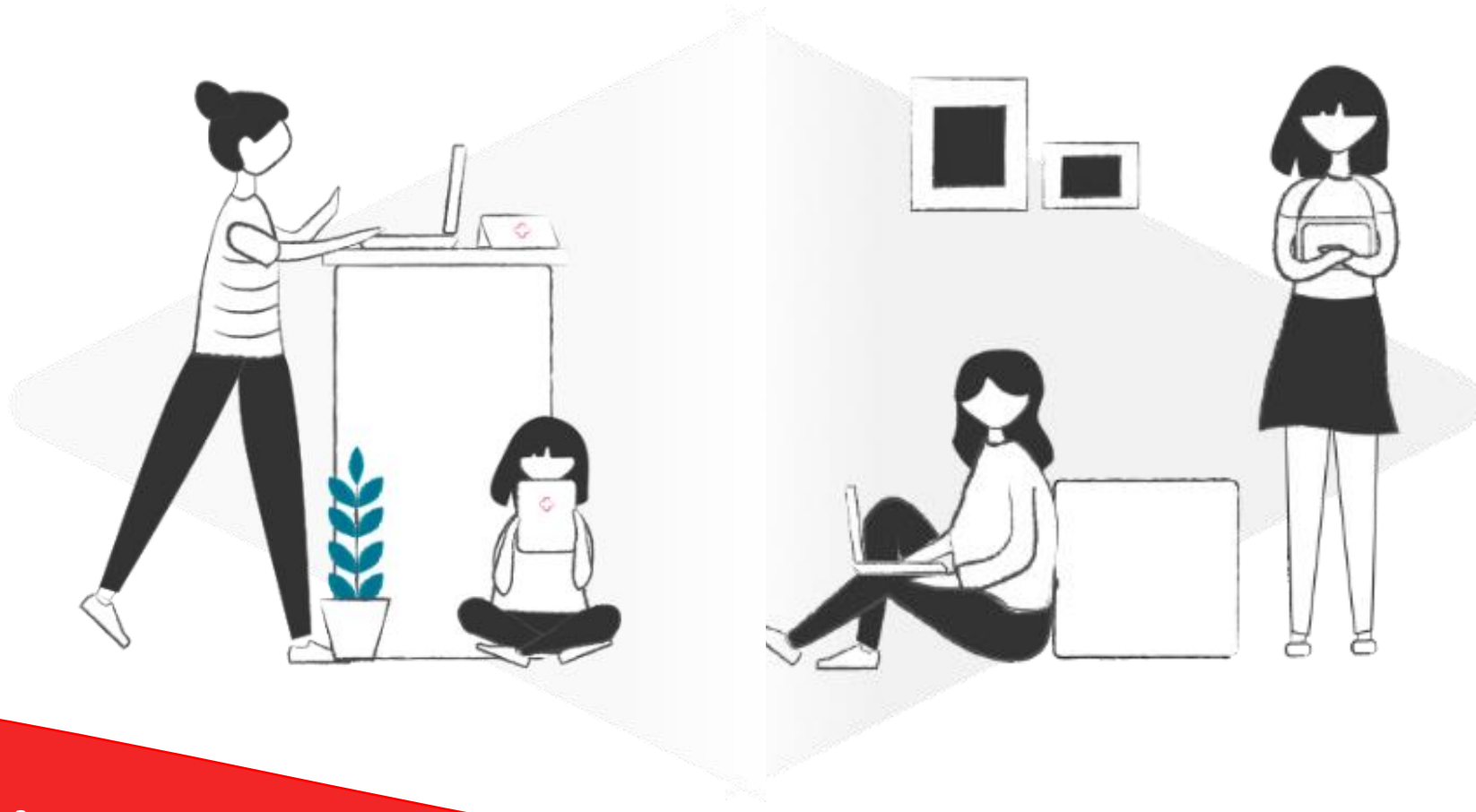
How to shop safely online

E-commerce has become the most popular way to shop, so knowing how to stay safe whilst making purchases online has never been more important. Find out the key things to look out for with our online shopping safety guide.

E-commerce Risks

The risks for online shoppers out there browsing through fraudulent websites and data leaks remains a persistent problem and threat. Online consumers are more at risk of accidentally buying fakes or replicas online due to trusting a photograph rather than inspecting the item in real life. Purchasing items that don't match the description, or goods that are damaged or unsuitable, is also a risk when it comes to making online purchases.

If you are browsing the internet using an unsecured Internet connection, such as a free Wi-Fi hotspot in a public place, then try to avoid making any online purchases. Public Wi-Fi is more vulnerable to attack by hackers or malicious software and could put you at an increased risk of fraud, so try to save any retail therapy for a night in!



How to tell if a website is safe?

There are many clues to identify whether a website is safe before making a purchase. Below are the features to be aware of when performing your own due diligence on e-commerce websites:

Check for a privacy statement

Look out for a privacy statement on any website you are planning to make a purchase from. A privacy statement detailing how the business collects, uses, and protects sensitive financial information should be readily available from any retailer – so if you're struggling to find one, this could be a bad sign.

Look for an address and phone number

Legitimate retailers almost always have a contact number and physical address visible in the header or footer of their website. If you have any reservations about the legitimacy of a website, copy and paste the address into an internet search engine to see if the given location is accurate. This is a good indication of a legitimate website, as unreliable sellers will often be online only to avoid detection, or use a fake address.

Check for an SSL Certificate

An SSL (secure sockets layer) is an encryption method that all online retailers who deal with credit or debit card details must have. **An SSL encryption stops hackers from accessing your personal or financial information, ensuring your details are secure and safe.** An SSL Certificate is a good indicator of trust and legitimacy on a website. There are two easy methods of determining whether a website has SSL certification. Firstly, an icon of a locked padlock should be present in the URL bar at the top of your web browser. Another method of identifying a website with an SSL Certification is the domain name:

- **Secure** websites begin with: **https://**
- **Unsecured** websites begin with: **http://**

Does the website accept credit cards?

Credit cards are the safest method of making online purchases, as it's easier for credit card companies to refund any money lost due to fraud. Websites that don't accept credit cards should raise a red flag, as it's often more difficult for fraudulent websites to become certified by credit card companies.

Try to use trusted retailers?

If possible, try to buy from retailers you have heard of, especially those with a reputation for customer service. If you're looking for a specialist item that is only available on an independent website, be as diligent as possible before handing over any financial information. Frequent spelling or grammatical errors in the product descriptions or website can be a good indication as to the quality of a website. Websites that appear to be written in broken English should be avoided, as well as websites that don't include unique photographs of the product, the ability to leave reviews, or an advertised returns policy.

Be suspicious of deals that are “too good to be true”

The saying that if something seems too good to be true, then it probably is, rings true when it comes to ecommerce safety. Be cautious of any website that appears to be selling well-known brands or designer items for considerably less than the retail price. If you discover a website that stocks popular items for very low prices, there's a risk you're handing over money for fakes or replicas. Common sense is usually enough to avoid being misled by these pitfalls. We would also recommend searching for the same item at different retailers to give you an impression of the average price.

Check out the reviews

While these tips can give you practical visual clues to look out for, reviews and personal accounts from other users are an excellent way of staying safe while shopping online.

Are you being asked to make payment away from the website?

Be suspicious when a website asks you to make a payment on an untrusted third-party payment platform. This is a very common form of crime, where hackers intercept the payment transaction and redirect it to a fake payment platform which they have access to. The original website may be fake, or in some cases genuine, but hackers have taken advantage of unsecure platforms by intercepting your transaction. The message is, buy on trusted websites with robust security measures in place.