FAQs for Safe Online Shopping

1. How do I stay safe while shopping online?

More and more shopping is being done online. The vast majority of online transactions are completed without any problems, but in some cases there are risks, and that's why we've created this page with useful tips and tools you can use in your online shopping.

If it's too good to be true

It usually is. Compare the price you're seeing with similar goods being sold elsewhere. If the price is significantly different, use caution - make sure to research the seller and ask questions about the condition of the item. When a site offers products that are heavily discounted, contains bad grammar and misspellings, and uses low quality images of the brand owner's official site, it might be selling counterfeit products. Be careful though, some sites selling counterfeit products mimic the brand owner's site by imitating the layouts and using similar images or using a domain name incorporating the brand.

Research unfamiliar sellers

If you haven't shopped from a merchant before, check beforehand to make sure they're legitimate. For example, learn more about their business history and do a web search for reviews from other buyers with experience with the seller. Legitimate merchants should provide you with contact information that you can reference if you have any questions or problems with your transaction, which may include a physical address, contact phone number, or email address.

Many sites selling counterfeit products will have official sounding URLs, which might include phrases like [brand]onsale.com or official[brand].com. Checking the site's WhoIs record is one way that might reveal who owns the domain.

Use a payment method with buyer protections

In many cases, credit card companies limit your liability for online purchases in cases of fraud. Some online payment systems do not share your full credit card number with sellers in order to give you extra protections.

Read the fine print

Before you purchase, make sure you're familiar with the seller's shipping, warranty, and return policy. Some stores will offer full refunds, while others charge restocking fees and give only store credit.

Keep a record of the transaction

Having a digital or paper copy of large transactions can help you if you do need to make a return or contest unauthorized charges made to your account.

Avoid hacked sites and keep an eye on the browser's address bar

If you click on a link and get instantly redirected, that site may have been hacked and contain malware. Malware, such as viruses, worms, and Trojan horses, can silently install

unwanted software on your computer. Some hacked sites won't automatically redirect you to a different page, but may contain irrelevant and spam-like content on the page. Keeping an eye on the address bar to ensure the link you click on is the one you are delivered to is one way to be vigilant.

Type sensitive web addresses into your browser's address bar

Don't navigate to sensitive accounts by clicking a link or copying and pasting the address. Instead, type out the web address yourself. But make sure that you're inputting the correct address; some typosquatting sites look exactly like the real site, but are set up to phish your account information.

Avoid entering personal information on suspicious sites.

If a site is asking for personal information beyond what is required to purchase a product or receive a service (e.g., bank account information, security question answers, or passwords) be suspicious as these types of inquiries may be indicative of a phishing attempt. Some sites may be a carbon copy of the official site, including logos and text, but are set up by fraudsters with the sole purpose of obtaining your personal information.

Here are some tips to avoid and report phishing sites:

Make sure your passwords are strong

Don't reuse passwords across multiple accounts, and remember to change them periodically, especially if you suspect your account may be at risk.

Only send information over secure connections

Look for the https:// connection in the address bar (and the padlock icon in your address bar if you're using Google Chrome or Internet Explorer) when transmitting any sensitive information like credit card or bank numbers. When accessing financial accounts, check that the website has an Extended Validation Certificate — the URL or website name should show up as green in the URL bar of many modern browsers, meaning the organization that operates the website has been validated.

Avoid conducting financial transactions on public computers:

Avoid logging into accounts that contain sensitive financial information (e.g. bank or credit card accounts or commerce websites) on public or shared computers. If you do access such information on a public or shared computer, remember to sign out completely and close your browser window after you're done.

Make sure you got what you paid for

Once you've received the item, give it a quick once-over to make sure everything is as it should be. The sooner you can try to address a case of fraud, the better chance you have to resolve it positively.