CARERS TRUST

GET SAFE ONLINE .org

www.getsafeonline.org

Keep your seasonal shopping safe this year

Holidays & Celebrations • Black Friday • Cyber Monday

Nowadays, most of us buy more online, and the run-up to our important seasonal celebrations is no exception. The thought of so much choice, being able to buy everything from the comfort of our armchair, finding a bargain and ultra-convenient home deliveries is too tempting to ignore. Let alone avoiding sore feet or having to find a parking spot.

However, online shopping does come with its own potential downsides. The holiday season, Black Friday and Cyber Monday also happen to be favourite occasions for fraudsters. Not only because this is the busiest time for people to go online to get their list ticked off or buy that last minute gift for someone special, or a treat for ourselves. But because they know that at this time of year, we can all be quite distracted, with so much going on.

Fraudsters exploit this and take advantage by using impersonation to persuade you into an action that enables them to steal your money or your identity, or both. However, you can take some simple precautions to protect yourself.

How do the scammers work?

They impersonate online retailers – from those large household names that sell everything to small, niche sellers – to persuade you to part with your hard-earned money with phishing emails, social media posts and messages and fake texts. You pay for the goods … *but there are no goods*. Or you click on a link – or open an attachment – only to find it leads to an authentic looking (but fake) website requesting personal details or laden with malware. To add another dimension, fraudsters are now making use of artificial intelligence (AI) to make their scams even more convincing.

You may have also heard about a number of other scams related to online shopping which vary in sophistication, which you can read more about at **www.getsafeonline.org/personal/blog-item/commonplace-online-retail-scams-and-how-you-can-avoid-becoming-a-victim/**

Top tips for buying safely online

- Make sure a website is authentic by carefully checking the address is spelled correctly. Ideally, type it in manually rather than clicking on a link in an email, text or post. It's easy for scammers to set up fake websites that are very similar to the real thing. You could check whether a website is likely to be legitimate or fraudulent at **www.getsafeonline.org/checkawebsite**
- Make sure payment pages are secure by checking that addresses begin with 'https' ('s' is for secure) and there's a closed padlock in the address bar. The https and closed padlock mean that the page is secure, but the site could still be operated by fraudsters.
- Social media sites/apps and online forums are a popular place for advertising gifts, tickets and holidays. Many are genuine, but you need to be aware that others are fraudulent. Be extra vigilant about checking that such ads are authentic, such as checking independent reviews and asking yourself if the price seems too good to be true.
- However desperate you are to buy that late present or an item that's in short supply, don't pay for it by transferring money to people or companies you don't know. If it's fraud, your bank may not be able to recover or refund your money. If you can, pay by credit card. The same goes for holidays, travel and tickets.
- Log out of the web page or app when payment is completed. Simply closing it may not log you out automatically.
- Do all you can to make sure you're buying genuine brands and not fake goods. Fakes or counterfeits are of inferior quality, contravene copyright law and affect the livelihoods of workers who make the real thing. They can also be unsafe in use.
- 'Low-cost' or 'free' trials can cause problems if you don't read the small print and look for independent reviews. Whether they're for the latest phone or a TV subscription service, you could be signing up for large monthly direct debits which are very hard to cancel.
- Learn how to spot fraudulent emails, texts, messages or fraudulent offers on social media. At this time of year, emails and other messages featuring 'special offers' and 'prizes' are commonplace. Don't click on links in emails, texts or posts that you're not expecting, and don't open unexpected email attachments.
- Text messages and emails claiming to be sent by home delivery firms are also commonplace, often informing you that there's a charge for re-delivering a parcel, or a shipping fee to be paid. However busy you are or how much online shopping you do, keep a record of everything you buy and, if possible, which parcel delivery firm the retailer is using.
- Check that seasonal breaks you book online are genuine by carrying out thorough research. Look for independent reviews, and make sure travel agents / tour operators are genuine by checking for an ABTA/ATOL number. This is normally listed at the very bottom of a website. It's always best to pay by credit card for extra protection.
- Get Safe Online has a range of tools that you can use to carry out safety checks before you transact online, at **www.getsafeonline.org/selfhelptoolcentre**

For more information on buying safely online, visit **www.getsafeonline.org**

Don't be put off!

We love the convenience and choice the internet brings, so please, don't be put off online shopping. Just take a few simple precautions as suggested above, and you'll stand a very good chance of getting what you want without any problems … perhaps except that latest toy being out of stock!

Happy shopping!

GET SAFE ONLINE .org

www.getsafeonline.org

CARERS TRUST