Don't get blue on Black Friday – the London Private Investigator advises...

Black Friday, once only seen in the USA, has recently become a UK staple in the run-up to Christmas. It's now a time when major retailers slash their prices to lure in enthusiastic and sometimes unsuspecting shoppers. Think of it as the mother of all January Sales come early. Traditionally it's the last Friday of November (25th this year), but some retailers have extended this to a week of crazy prices starting tomorrow.

Great. A chance to get some Christmas presents at a bargain price. What could possibly go wrong?

As it happens, quite a lot. Whilst this experienced private investigator does not wish to appear po-faced, it's important that as ever we offer you some words of wisdom.

The main problem is that lots of these Black Friday bargains are only to be found online. The high street shops spend a fortune targeting buyers for their once in a lifetime deals. Sitting in the comfort of your own home, perusing the online offers,

you'll be bombarded with suggestions persuading you to part with your hard-earned cash. If you're a savvy shopper with a hard nose for a bargain coupled with a natural suspicion of Too Good to be True deals, you'll probably do quite well.

But it's predicted that 6.5 million cyber attacks will take place around Black Friday week. Think about it: for the unscrupulous fraudster, this is a golden opportunity - millions of shoppers all online at the same time, many of whom perhaps don't use the internet that often but are seduced by the lure of a bargain. For the criminal, that is a perfect storm.

So what can you do to prevent yourself losing money to online fraudsters? First of all, beware of the adverts purportedly coming from online retailers on social media. We've all see adverts like this on Facebook and Twitter and most of the time they are genuine. But on Black Friday there is a massive increase in fake sites, all trying to get your money. Genuine sites should always have a blue tick on their profile page which means that they have been verified as being bona fide. If you are still not sure, use the company's normal website to make purchases, and when you get to the payment page, make sure the URL begins http**s –** it's the “s” that is important here. S = Secure.

Secondly, treat all emails coming from online retailers with suspicion, especially if they are unsolicited. It's normal to get emails from retailers if you have made purchases from them before or you have an account, but unsolicited emails should always be viewed with caution.

You also need to look carefully at the language used in email offers and online adverts on social media. Fraudsters are notoriously bad spellers! Check the English carefully – are there spelling and grammar mistakes? If so, don't go there. Major, genuine retailers have an army of proof readers checking their content, so it's unlikely to be genuine if it's badly written.

Finally, normal common sense rules of the internet apply – don't click on attachments unless you're 100% sure they are genuine; if you're invited to click on a link, hover over the URL to see where it takes you – if in doubt, don't click; delete any suspicious emails straight away and block the sender and make sure you have up-to-date anti virus software.

Have a happy Black Friday bargain hunters! From Anderson Chance, the recommended Private Investigator of choice.

www.andersonchance.com