

Alresford and District Neighbourhood Watch Association



This year Christmas will be different. More of us than ever will be buying presents and other seasonal goods on the internet. But with the Covid-19 pandemic still very much with us, we have more on our minds than usual, making us easier targets for online fraudsters. So, before you start your Christmas shopping in earnest, please take a few minutes to read these easy-to-follow tips from *Get Safe Online's* experts to help save you from giving a fraudster an early Christmas present.

However, if you're reading this after you have done your Christmas shopping on-line, please don't stop reading! Much of the advice below is valid throughout the year.

- When you're shopping online, **make sure websites are authentic** by carefully checking the address is spelled correctly. Ideally, type it in 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.
- When you're paying, make sure the page is secure by checking that addresses begin with 'https' ('s' is for secure) and there's a closed padlock in the address bar. However, word of warning: this only means that the page is secure, but the site could still be operated by fraudsters.
- Many advertisements for items such as gifts, holidays and events on social media and online forums are genuine but be aware that others are fraudulent. Be extra vigilant about checking that such ads are authentic.
- However desperate you are to buy that late gift or an item that's in short supply, don't pay
 for anything by transferring money directly to people or companies you don't know. If it's
 a fraud, it's doubtful the bank will 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.
- **Fake or counterfeit goods** are of inferior quality, contravene copyright law and affect the livelihoods of workers who make the real thing. They can also be dangerous to users. Don't buy them intentionally however cheap or 'authentic' they appear and do all you can to make sure what you're buying is authentic.
- **Avoid 'free' or 'low-cost' trials** whether for the latest handset or slimming pills without thoroughly reading the small print and trusted reviews. You could be signing up for large monthly direct debits which are extremely hard to cancel.
- Christmas is a favourite time for scammers to send fraudulent emails, texts or direct
 messages or post fraudulent offers on social media. Also, with the increase in internet
 shopping, fake parcel firm delivery notifications are commonplace with attachments or links, as
 are emails and other messages featuring "special offers" and "prizes". Don't click on links in
 emails, texts, or posts that you're not expecting, and don't open unexpected email
 attachments.

If anyone has suggestions for topics that they think would be suitable for future Neighbourhood Watch articles in the Forum, please get in touch - e-mail <u>contact.adnwa@gmail.com</u>