

Information supplied by the Thames Valley Police

In the immediate run up to Black Friday, Cyber Monday and Christmas 2020, the National Cyber Security Centre and Action Fraud have launched their own mini campaigns to help provide guidance to UK residents to shop securely online and to fight back against Fraud this Christmas.

The National Cyber Security Centre has said: <https://www.ncsc.gov.uk/blog-post/shop-securely-online-this-black-friday>

With Black Friday and Cyber Monday fast approaching, it's likely that shoppers will move online more than ever with most high street stores still closed. We have [updated our online shopping guidance this week](#) to give you the most up to date advice on how to stay secure whilst getting the best deals online.

The refreshed six steps in this guidance will help you to avoid scam websites and purchase items securely:

1. Choose carefully where you shop
2. Use a credit card for online payments
3. Only provide enough details to complete checkout
4. Keep your accounts secure
5. Watch out for suspicious emails, calls and text messages
6. If things go wrong

By following our shopping online securely guidance we hope that we can help you avoid scams and instead focus on bagging a bargain.

Action Fraud has laid out: <https://www.actionfraud.police.uk/news/action-fraud-launches-new-campaign-to-fight-back-against-fraud-this-christmas>

Action Fraud's #FraudFreeXmas campaign has launched today, with a stark warning about 'too good to be true' Black Friday deals. Figures reveal reports of online shopping fraud have surged by 30% over the pandemic as many of us continue to shop online in light of current restrictions

Figures from Action Fraud show that criminals conned 17,407 shoppers out of almost £13.5 million over the Christmas period last year, an increase of over 20% when compared to the same period in 2018. Action Fraud is warning the public to take extra care when shopping online, ahead of Black Friday and Cyber Monday, as shoppers search for bargains and gifts for loved ones in the run up to Christmas.

Thames Valley Police Advice

Thames Valley Police will be circulating guidance and advice relevant to the above campaigns via external facing social media outlets, of which our @TVPCyber_Fraud Twitter account is one.

Watch out for phishing emails or texts: Some of the emails or texts you receive about amazing offers may contain links to fake websites. If you're unsure, don't use the link and visit the website directly instead. If you receive an email you're not quite sure about, you can report it by forwarding the email to the Suspicious Email Reporting Service at report@phishing.gov.uk. You can report suspicious texts you have received by forwarding the original message to 7726.

When things go wrong: Anyone can fall victim to fraud. If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online at [actionfraud.police.uk](https://www.actionfraud.police.uk) or by calling 0300 123 2040.