The Fraud & Scam Bulletin

DECEMBER 2025

Your monthly update direct from West Mercia Police on the latest scams and frauds

CHRISTMAS SHOPPING

No sooner has the threat of Black Friday passed, that we enter the full-on Christmas shopping period, and once again the criminals will want to tempt the unwary online with those “too good to be true” offers.

So, what are the options, face the crowds in the shopping malls, or relax at home and do the Christmas Shop online?

Whilst the internet is the first port of call for Christmas Gift bargains for many in terms of speed, convenience and savings, it also provides a great opportunity for Fraudsters to profit at your expense.

Even when you have been wary throughout the year with your online shopping, it can be so easy to be caught out in the heat of the moment in the rush up to Christmas when our minds are elsewhere, or just too busy to carry out a check to see if that “bargain” really is a bargain.

Also, beware of those Phishing emails claiming to be from genuine charities and playing on the season of goodwill. They may even display seemingly genuine logos for national charities, such as Red Cross or Salvation Army, but the charity will never see your money.

So always go directly to the chosen charity’s website to donate, and always beware of door to door, and street collectors if they cannot show genuine identification for the actual charity. So once again, it is safer to donate to that charity direct.

Therefore, once again, please make family members aware, particularly those in the vulnerable age groups. Especially be mindful when shopping on Social Media platforms, as this is by far the most likely medium for shopping and auction frauds to take place.

HOW TO STAY SAFE

So online shoppers are urged to protect their accounts. Do use secure payment methods to stay ahead of the threat from fraudsters who are particularly active with the build-up in Christmas shopping online.

- Protect your accounts: set up **2-step verification** and use **3 Random Word passwords** to prevent Cyber criminals gaining access to any of your accounts (see Three random words - NCSC.GOV.UK)
- Be wary about where you shop online – check out Online Retailers, especially ones you have not used before and make sure they are legitimate
- Don't pay for goods or services by bank transfer unless you know and trust the person. Payments via bank transfer may not offer you sufficient protection if you become a victim of fraud.
- Pay Securely: use a Credit Card when shopping online as most major Credit Card companies protect online purchases. Also using a Credit Card rather than a Debit Card means your main bank account will not be affected if your details are stolen.
- Whenever you pay always look for the "*Closed Padlock* "symbol in the web address bar showing your connection is secure
- Finally, Do not let Christmas come early for criminals and fraudsters

Please feel free to share these messages with any vulnerable friends, relatives or neighbours.

If you have been a victim of fraud

Report it to **Action Fraud on 0300 123 2040** or via actionfraud.police.uk

Scam Text messages can be forwarded to 7726 to help phone providers take prompt action and block numbers that generate spam on their networks.

You can also report fraudulent mobile calls by texting **7726** with the word **"Call"** followed by the **fraudster's phone number**.

Scam calls received on WhatsApp can be blocked by opening the chat with the suspect phone number and tap on "Block".

Forward **Fake Emails** received to **report@phishing.gov.uk**

If you think your bank account or personal banking details have been used fraudulently, then use the short phone number **- 159** - to contact the Fraud Prevention Department of most major UK banks.

West Mercia POLICE