THAMES VALLEY POLICE

TV Alert

Don’t let fraudsters dull your sparkle this festive season

The run-up to the festive season is often a whirlwind—exciting, but also stressful. With the added hustle and bustle on top of everyday demands, it’s easy to feel pressured to act fast and make quick decisions.

Unfortunately, fraudsters are counting on this. They exploit the chaos to their full advantage, turning festive cheer into empty bank accounts, financial strain, and shattered plans.

The good news? The Central Fraud Unit at Thames Valley Police has put together top tips to help you keep the season merry and bright—free from the fear of fraud.

Detective Inspector Duncan Wynn, Head of Central Fraud Unit said:

“With major shopping events like Black Friday and Cyber Monday now spanning several days, consumers are inundated with offers that often seem too good to be true. Last year alone, £11.8 million was lost to online shopping fraud during the festive season.

While there are certainly genuine bargains out there, I strongly urge the public to stay vigilant and take extra care when hunting for deals.”

There are 3 key areas of focus which can help disrupt the fraudster’s plans and keep our festive plans on track.

Research sellers to check they are legitimate

You can check whether an online shop is legitimate—especially if it’s one you haven’t used before—by researching it first. Look for reviews on trusted consumer websites or from people and organisations you know you can rely on.

THAMES VALLEY POLICE

TV Alert

Be alert for suspicious emails or text messages (known as phishing) that include links to fake shopping sites offering deals that seem too good to be true. Criminals can easily copy the design of genuine websites, including logos, trademarks, and product images. They often use deceptive web addresses, such as **www.tescos-sales.com**, which can look similar to the real domain **www.tesco.com**.

If you're unsure about a link, don't click it. Instead:

- Type the official website address directly into your browser's address bar (if you know it).
- Search for the organisation online and take time to review the search results—don't just click the first link.

If you receive a suspicious email, report it by forwarding it to phishing@report.gov.uk

Suspicious SMS/text messages can be forwarded to 7726, which spells out 'SPAM' on the telephone keypad.

Use a credit card or secure payment platform

Whenever possible, use a credit card for online payments. Credit cards often provide additional protection under the Consumer Credit Act.

Debit cards offer less protection, but you may still be able to request a refund through a voluntary scheme known as 'chargeback'.

If you choose payment services like PayPal, Apple Pay, or Google Pay, review their terms and conditions to understand what buyer protection they offer.

Never pay by direct bank transfer—it offers no protection and is a common method used by fraudsters.

Only provide required details on checkout

When making a payment, only provide the essential details—usually marked with an asterisk—such as your address. Unless you plan to shop regularly with the retailer, avoid creating an account. Instead:

- **Choose 'Guest Checkout'** whenever possible, so you don't need to register to complete your purchase.

- **Use secure payment platforms** like PayPal, Apple Pay, or Google Pay, which typically allow you to pay without creating a store account.
- **Don't allow your browser to save payment details** if prompted.
- If you do create an account, **never store your bank or card details for future purchases**—it's safer to enter them each time.

Detective Inspector Duncan Wynn, continues:

"In addition to the steps already mentioned, I strongly recommend strengthening your online security by enabling 2-step verification on all important accounts. This extra layer of protection makes it significantly harder for fraudsters to gain access.

Criminals often use psychological tactics to push us into a 'hot state'—a moment where emotions override rational thinking and lead to impulsive decisions.

Taking a moment to Stop! Think Fraud gives us the space to pause, reflect, and help minimise the risk to ourselves and others.

By looking out for those around us too, we can all do our bit to aim for a fraud free festive season"

Further steps on how to minimise the risk of fraud can be found in the Fraud Protection toolkit which is an exclusive publication by the Central Fraud Unit, focusing on each route of contact fraudsters exploit.

The Central Fraud Unit also run an account on 'X', packed full of essential fraud protect advice. Follow @TVPCyber_Fraud

If you have been a victim of fraud, notify your bank immediately and report it to Action Fraud at actionfraud.police.uk or by calling 0300 123 2040. Always call 999 in an emergency.

You can also contact Crimestoppers anonymously on 0800 555 111.