Fraud Alert

Online Christmas Shopping Fraud

tiaa

Staff are being advised to take extra care when shopping online in the run up to Christmas.

Figures released by Action Fraud show that online fraud was responsible for losses of almost £13.5 million over the Christmas period last year, an increase of over 20% when compared to the same period in 2018. Evidence of this trend can already be seen, as UK Finance reported over £27million was lost to fraud at online marketplaces and auction websites in the first half of 2020, averaging at a loss of £720 per case.

The outbreak of coronavirus earlier this year, and the restrictions that have been introduced have caused many people to turn to online shopping and banking for the first time. Consequently, reports of online shopping fraud have surged by 30% over the pandemic as many shop online in light of current restrictions.

Status: Action Required

This alert provides information and advice to staff about fraud and economic crime, and the risks associated with it.

If you have fallen victim to fraud or cyber-crime you should report it to Action Fraud by calling 0300 123 2040, or visiting: https://reporting.actionfraud.police.uk/

How to protect yourself from fraud

- Carry out some research first, or ask a friend or family member if they've used the site and about their experiences before completing the purchase.
- Only create an account if necessary. Be cautious if the website asks you for details that are not required for your purchase, such as your mother's maiden name or the name of your primary school.
- Ensure that the webpage where you enter your payment details is secure (website address starts with "https").
- Revisit password habits. The length and strength of a password, combined, is the strongest deterrent to a hacker.
- Take advantage of additional authentication features. The easiest type to use is a one-time use passcode, which can be texted, emailed or pushed via an app.
- Use a credit card to pay online. If the worst should happen, your main bank account won't be directly affected or use well established methods like PayPal, Apple Pay and Amazon Pay when buying on auction site.
- Some of the messages or emails you receive may contain links to fake websites. If you are unsure, don't use the link - go separately to the website.
- Staff should monitor their credit reports and their finances. Not just to stay informed about credit history, but also to spot anything suspicious as quickly as possible.

For further discussion and support, including fraud awareness training services, contact:

Melanie Alflatt
Director of Fraud and Security

T 0845 300 3333
E fraudsmart@tiaa.co.uk

FRAUD SMART