Keep Your Money Safe

Surrey Police and Sussex Police Fraud Newsletter

In this issue:

Stay safe from online shopping fraud this festive season

Residents are being warned about a sharp rise in an emerging trend of Amazon impersonation fraud.

Upcoming Community Engagements

"Each month we see many incidents of fraudsters targeting our residents in an attempt to defraud them. We're working hard to prevent this and support vulnerable victims of fraud or scams. By following our tips and encouraging family, friends and colleagues to do so too, you can reduce the risk of becoming a victim."

Detective Chief Inspector
Paul Driscoll
Surrey Police &
Sussex Police
Economic Crime Unit

STAY SAFE FROM ONLINE SHOPPING FRAUD THIS FESTIVE SEASON

As Black Friday, Cyber Monday and the Christmas shopping season approach, many people will be searching online for gifts and special offers. While online shopping is convenient, it is also a time when fraudsters increase their activity, targeting both buyers and sellers through fake websites, deceptive adverts and convincing messages.

Online criminals use a range of tactics to steal money and personal information. They often create professional-looking websites and social media adverts offering popular products at heavily discounted prices.

In other cases, shoppers may receive counterfeit goods or nothing at all after making a payment. Fraudsters also send emails and text messages that appear to come from trusted retailers or delivery companies, encouraging recipients to click links or provide personal information.

Be aware if you are selling items online, you may also be targeted by payment scams designed to obtain money or goods without legitimate payment being received.

If your group or organisation would benefit from a free, tailored fraud prevention presentation or an in-person engagement session, please contact the Sussex and Surrey Fraud Prevention Team at SussexandSurreyFraudPreventionEngagements@surrey.police.uk for further information.

What to Look Out For:
Be cautious of prices that seem significantly lower than those offered elsewhere, particularly on products that are in high demand.

Take time to check websites carefully and be wary of poor spelling, low-quality images, limited contact details or recently created social media accounts.

Unexpected emails, texts or messages about orders, deliveries or special offers should be treated with caution, especially if they contain links or request personal or financial information.

Fraudsters frequently create a sense of urgency to encourage quick decisions before someone has time to verify whether a request is genuine.

Shopping Safely Online
Using familiar and reputable retailers can help reduce the risk of fraud. Where possible, access websites directly rather than through links in emails, text messages or social media adverts. Before making a purchase, take a few moments to research the seller and read independent reviews.

Paying by credit card, debit card or a trusted payment service can provide additional protection compared with bank transfers.

Keeping devices updated with the latest security software and using strong, unique passwords can also help protect accounts from unauthorised access.

For those selling items online, it is important to ensure payments have been received and cleared before dispatching goods.

Be cautious of requests to move conversations away from secure selling platforms or to use alternative payment methods.

If an offer appears unusually attractive, a seller is rushing you to make a payment, or a message requests personal or financial information, take a moment to pause and verify the details independently. A genuine retailer, delivery company or online marketplace will not mind if you take time to check.

Reporting Suspicious Activity
Suspicious emails can be forwarded to report@phishing.gov.uk, and scam text messages can be reported free of charge by forwarding them to 7726.

Online shopping should be enjoyable and stress-free. By taking a few simple precautions and remaining alert to unexpected messages, deals and payment requests, you can help keep yourself, your family and your finances safe throughout the festive season.

Join Report Fraud's free webinar "Online Shopping: Protect yourself this Festive Season" on 23 November, 10:00am to 11:00am, where you'll hear practical advice on how to shop safely online, spot common scams, and protect yourself from fraud.

Learn how to recognise warning signs. Find out how to shop securely online. Get advice on avoiding common fraud tactics.

Register here: https://orlo.uk/NXEUG

Residents are being warned about a sharp rise in an emerging trend of Amazon impersonation fraud.

Criminals contact people unexpectedly, claiming there has been suspicious activity on their Amazon account. They often say unauthorised items have been added to the victim's basket and provide fake delivery addresses to make the scam appear genuine.

Fraudsters then convince victims that urgent action is needed to secure their account and prevent payments from being taken.

In a recent case a vulnerable male from Surrey was deceived into transferring over £1000 to fraudsters claiming his Amazon account had been hacked and there were items in his basket. To stop the ‘hacker’ he was told to download the AnyDesk and Western Union apps which is how the scam then played out.

Two females from Sussex were also defrauded in this way, both being contacted initially by telephone and in turn losing hundreds of pounds each to the fraudsters.

How the Scam Works
Victims may be instructed to:

- Share their screen via a messaging app, allowing criminals to gain access to online banking.
- Download money transfer or remote access software, enabling criminals to move money or take control of devices.
- Provide identification documents such as passports or driving licences for supposed "verification" purposes.
- Authorise payments to stop alleged purchases or gift card transactions, when the money is actually sent to fraudsters.

Remember: Amazon, your bank and the police will never ask you to transfer money, download remote access software, share security codes, or give someone control of your device.

If you receive a call or message that doesn't feel right:

- End the call immediately.
- Contact Amazon or your bank using contact details from their official website or app.
- Never trust caller ID alone, as it can be spoofed.

Amazon's resources & tips
Please see Amazon's latest Trustworthy Shopping Experience Blog post:
https://trustworthyshopping.aboutamazon.com/en-uk/amazon-scam-trends

You can also find tips to help you spot and avoid scams impersonating Amazon:
https://www.aboutamazon.com/news/retail/how-to-avoid-amazon-scams

Upcoming Community Engagements

If you would like to meet our dedicated Fraud Prevention Volunteers, we would be delighted to see you at one of our upcoming community engagement events. Our team will be on-hand to answer any fraud-related questions and provide practical advice and support.

Tuesday, 17 November 10:00am to 2:00pm - The Friary Centre, Guildford (outside Sostrene Grene) Representatives from Surrey Police, PCC Lisa Townsend and partner organisations will also be in attendance.
Tuesday, 24 November -Elmsleigh Centre, Staines
Wednesday, 25 November - The Belfry, Redhill
Thursday, 26 November (morning) - Waitrose Community Café, Dorking

Thursday, 26 November - Molesey Xmas lights turn on
Tuesday, 8 December 10:00am to 12:00pm - Holmbush Centre, Shoreham