Keep Your Money Safe

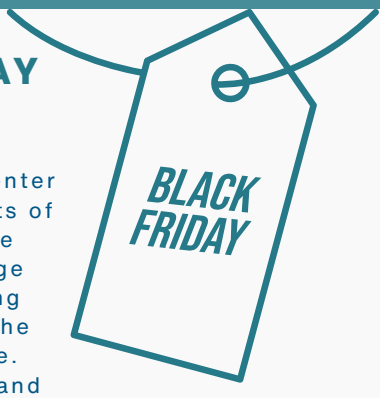
Surrey Police and Sussex Police Fraud Newsletter

In this issue:

"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."

T/Detective Chief Inspector Antony Leadbeatter, Surrey Police & Sussex Police Economic Crime Unit

BLACK FRIDAY AND CYBER MONDAY ARE COMING...



Past seasonal trends tell us to expect, that as we enter the festive period, it is likely incidences and reports of online shopping fraud will increase. With the festive period fast approaching, shopping habits will change with many looking to 'bag a bargain' online. Amazing offers and price slashed deals designed to lure in the shoppers can sometimes appear too good to be true. High profile shopping events such as Black Friday and Cyber Monday centre around these and is something fraudsters will exploit.

SHOP SAFELY WITH THESE TIPS:

1.Check the shop is legitimate
You can research online shops to check they're legitimate, particularly if it's a store you've not used before. Use consumer websites, or reviews from people (or organisations) that you trust.

2.Use a credit card to pay
Use a credit card for payments (if you have one). Many of these protect online purchases as part of the Consumer Credit Act.

3. Only provide required details on checkout
When making your payment, only fill in the mandatory details (often marked with an asterisk) such as your address. Unless you think you'll become a regular customer, don't create an account for the store.

4.Keep your accounts secure
Make sure your shopping, online banking and payment accounts are protected by strong passwords that you don't use for any other account. If you're using the same password for lots of accounts, criminals could steal your password from one account, and use it to access your other ones.

KEEPING YOUR TECH SAFE

It's very safe to say that technology isn't going anywhere... and with Christmas coming, you might be hoping to get your hands on some brand-new tech!

REMEMBER: Software updates aren't just for new features or a pretty new home screen. They repair bugs and resolve security vulnerabilities. If possible, you should enable automatic updates on your personal devices to make this process more streamlined and easier for you.

THINK – BACKUPS: Imagine how devastating it would be if you lost your phone and with it all your photos and contacts' details, just because that data hasn't been backed up somewhere.

Microsoft and Apple both offer a small amount of cloud storage (online) for free that can be used to store backups, or you could use an external hard drive/USB stick.

DEEPFAKE INVESTMENT SCAMS

Sussex and Surrey Police have seen an increase in reports from victims being lured into investment frauds through the use of a fake celebrity profiles.

Below we describe two cases which involve adverts where trusted celebrities have endorsed the companies, however, deepfake technology has been used to create these fake videos, and the celebrities have nothing to do with them. Other celebrities used in similar scams include Chris Tarrant, Ben Fogle, Elon Musk, and US podcaster Joe Rogan.

Robert Peston Deepfake

A Surrey man in his 60's was browsing social media when he saw an advert where Robert Peston, the ITV Political analyst and commentator was seen recommending a crypto currency investment opportunity. As Robert Peston is a respected and trusted celebrity, he called the number on the advert. After several months of convincing interactions in what would later transpire to be a long and convoluted scam the victim was left £150,000 out of pocket.

Martin Lewis Deepfake

In Sussex, an elderly lady was browsing the internet when she saw a video with Martin Lewis, the Money Saving Expert, explaining how he was making millions investing through a company, who used AI (Artificial Intelligence) and advanced technologies to make informed decisions that are making their investors millions.

As Martin Lewis is a celebrity focussing on consumer advice and is someone she trusted, she decided to contact the company he was promoting and filled out an enquiry form. What followed was again a complex, and drawn-out fraud, using convincing communications, impersonations, and technology. After losing £3000 to this fraud, sadly the lady was left feeling embarrassed and out of pocket and incredibly upset. On reporting this to Sussex Police she was provided with support, access to services and fraud prevention advice.

PROTECTING YOURSELF FROM INVESTMENT FRAUD

1.Resist pressure to commit quickly: Scammers often want you to act fast.

2.Research investment programs: Search online for reviews, scams, fraud, or complaints related to the company or program.

3.Verify investment claims on your own: Do not rely solely on what you're told.

4.Know the risk: Understand the risks associated with any investment opportunity.

5.Get a second opinion: Be sceptical of unsolicited investment opportunities.

6.Check registration: Ensure that anyone selling or offering investment advice is registered with the FCA.

7.Take the time you need: Be cautious of time-limited offers and high-pressure salespeople.

8.Research the investment: Investigate thoroughly before committing.

WINTER FUEL PAYMENTS

Due to the recent changes in payments for Winter Fuel and Household support funds, we have seen an increase in phishing texts and emails purporting to be from the DWP stating that you may be entitled to claiming for these by clicking on links to update information.

Never click on links from untrusted sources. They may take you to convincing looking web pages which are set up to steal your data and could then be used for criminal activity.

Top Tips:

Local authorities will never text or call you to ask for your bank details in relation to welfare support.

Never click on untrusted links in texts or emails.

Research if these messages have been received by others.

If you are eligible for either of the payments above, you will be notified automatically.

If you receive a suspicious text or email, please report it.

You can report through the suspicious email reporting service at Report@phishing.gov.uk or the suspicious call or text reporting service on 7726.

NEW YEAR, NEW CHALLENGE

FRAUD PREVENTION IN THE COMMUNITY – IS THIS A VOLUNTEERING ROLE FOR YOU?

We are looking for volunteers to join our existing Volunteer Fraud Prevention Programme in 2025 in an exciting newly developed role as Community Engagement volunteers. The volunteers will work alongside our Neighbourhood Policing Teams based in local Police stations, delivering fraud prevention advice and guidance to the residents of Sussex.

This will include engaging with the public in a variety of different settings such as delivering fraud presentations and attending events / key locations to hand our fraud prevention literature and provide advice and education to the public e.g. farmers markets, community centres, libraries etc.

If you feel this is something that you would like to be involved with, please complete the application here.