



Keep your money safe

Surrey and Sussex Police Fraud Newsletter March 2020

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 Andy Richardson, Surrey & Sussex Police
Economic Crime Unit**

Be vigilant when using cash machines

We've seen a spate of reports of cash machine scams in recent months. The scam begins when victims attempt to withdraw money and discover the cash machine is faulty – it either seizes up or swallows their card.



There have been several variations on what happens next. In one case, a man in a hi vis jacket advised the victim to press various buttons on the machine. The machine still did not seem to work but the victim then noticed the man go to a nearby machine and withdraw a 'handful' of cash. The victim later found out the man had somehow managed to

Keep your money safe

take £500 from their account. In another case, a man offered to call the bank from his mobile to report that the victim's card had been swallowed. After dialling, he passed his phone to the victim, who spoke to a 'very reassuring' man who said someone would be out within 30 minutes to retrieve her card. No one turned up. Later that day the victim found out her card had been used for £5000 worth of payments.

Keep your money safe. Our advice is to:

- Scan the area around cash machines before you use them, checking for anything unusual
- Be aware of anyone near you, especially if they try to distract you while you're using the machine
- Shield your PIN
- Put your card away immediately
- If possible, use an ATM inside a bank

Loft and roof insulation fraud

This is another fraud that we saw a spike in last month. In most cases, victims are called by a company claiming that their roofing insulation is not sufficient and needs assessing. In some cases the callers suggest that they are offering a government backed scheme. If the person declines the offer, the caller attempts to make a booking for someone to come to the victim's house and assess their insulation (which will provide the fraudsters with another opportunity to pressure their victim into parting with money.)

Luckily, in most cases we've seen no one has lost any money. Let's keep it that way. If any one cold calls you about insulation, or any other subject for that matter, please remember our advice:

- Never give money to anyone you don't know or trust
- Check people are who they say they are
- Don't share your personal information
- Make decisions in your own time

Fraudsters exploit coronavirus

Fraudsters are exploiting the spread of coronavirus to commit fraud and cybercrime.

Since February 2020, the National Fraud Intelligence Bureau (NFIB) has identified 21 reports of fraud where coronavirus was mentioned, with victim losses totalling over £800,000. Ten of these reports were made by victims that attempted to purchase protective face masks from fraudulent sellers. Reporting numbers are expected to rise as the virus continues to spread across the world.

Fraudsters are also sending out coronavirus-themed phishing emails in an attempt to trick people into opening malicious attachments or revealing sensitive personal and financial details.

Keep your money safe

Some of the other tactics reported include fraudsters purporting to be from research organisations affiliated with the Centre for Disease Control and Prevention (CDC) and the World Health Organisation (WHO) contacting potential victims over email. They claim to be able to provide the recipient with a list of coronavirus infected people in their area. In order to access this information, the victim needs to click on a link which leads to a malicious website, or is asked to make a payment in Bitcoin.

Watch out for scam messages:

Don't click on the links or attachments in suspicious emails, and never respond to unsolicited messages and calls that ask for your personal or financial details.

Shopping online:

If you're making a purchase from a company or person you don't know and trust, carry out some research first, and ask a friend or family member for advice before completing the purchase. If you decide to go ahead with the purchase, use a credit card if you have one, as most major credit card providers insure online purchases.

For more information on how to shop online safely, please visit:

<https://www.actionfraud.police.uk/shoponlinesafely>

How you can help us

If you or someone you know is vulnerable and has been a victim of fraud call:

Surrey Police on 101 or visit www.surrey.police.uk

Sussex Police on 101 or visit www.sussex.police.uk

Report fraud or attempted fraud, by contacting Action Fraud at

http://www.actionfraud.police.uk/report_fraud or call 0300 123 2040