Sussex Police fraud newsletter – May 2017

Keep your money safe

Each month, we see many incidents of fraudsters targeting Sussex residents in an attempt to defraud them. Operation Signature is our answer to preventing and supporting vulnerable victims of fraud or scams.

By its very nature, fraud is constantly evolving and taking on new forms. By following our tips and encouraging family, friends and colleagues to do so too, you can reduce the risk of becoming a victim.

This month we focus on case studies of people preyed on by someone pretending to be from your bank or a reputable company – who try to convince you to tell them your bank details over the telephone.

Detective Chief Inspector Steven Boniface, Operation Signature, Sussex Police

TalkTalk

We have seen several cases of fraud in Sussex over the past few months, relating to TalkTalk customers. A phone call claiming to be from TalkTalk told a resident that there were problems with their wireless router and the caller asked for remote access to his computer so that he could display an error message on the screen. The fraudster said that they would be replacing the router and that he would get a compensation payment of £200. The resident gave his online banking details including account number and sort code. The fraudster then asked him to check that the correct amount had been deposited and that the online bank statement showed that £5200 had been paid in. The fraudster said that the £5000 had been an error and requested that the person pay back £4900 - leaving an extra £100 as a gesture of goodwill for the error made.
Later that afternoon, the victim received a call from the bank to say that there had been fraudulent activity on his account. The bank have offered him £75 compensation in recognition of the money he has lost through the fraudulent activity, but he is now £4825 out of pocket.

Microsoft

An elderly woman received a telephone call from a man calling himself ‘Peter Robinson’ from Microsoft who said her computer was hackable by terrorists. He said that if she didn’t send money, she would be reported to the police who would arrest her. She was told that Microsoft would give her £500 in compensation, but it required them to send £4500 and she should send them £4000. The money was sent using Western Union. The victim, although well aware of scams that take place over the phone and by mail, was unfamiliar with online fraud.

Sussex Police fraud newsletter – May 2017

BT

This fraudster advised a man he was from the BT Technical team saying hackers were active on the resident's phone line, and wanted his assistance in getting them arrested. They asked for his bank account details to allow them to transfer £1000 to him, which the man provided. The resident was told to transfer £800 pounds via MoneyGram to a 'Mr Hadjie,' which was stopped by staff when he was carrying out the transfer at a MoneyGram terminal.

Courier fraud on the rise in Sussex

Courier fraud crime involves fraudsters posing as bank staff or as in this case, a police officer. They phone to persuade you that your bank account has been hacked or that they need your help to catch organised crime gangs. They tell you to withdraw money and hand it to one of their trusted associates - the courier - who will either keep it safe or use it in their fake police operation. Sussex Police saw a rise in this deception method and others two years ago and worked with the banks to identify unusual or suspicious cash withdrawals.

A local 85 year-old woman from Chichester handed over £12,500 after a man claiming to be from the 'Metropolitan Police Fraud Squad' said that her bank card had been copied and she needed to withdraw £5,000. She went to her bank, withdrew the cash and handed it to a courier who arrived at her house during the afternoon. The man then phoned her back asking her to withdraw £7,500 and again hand it to a courier, which she did. She became suspicious and it was reported to the police. We want to raise awareness of this scam and would urge people to be vigilant. No official organisation would ever make calls like this and would never ask for you to withdraw money from your account.

DVLA vehicle tax refund fraud

Police are warning residents in Sussex not to be taken in by 'cold caller' text messages suggesting they are due a DVLA vehicle tax refund. An unsuccessful attempt was made in Worthing late last month but police are aware that that there have been some similar reports elsewhere in the county. The resident had a text message which claimed he was owed a DVLA vehicle tax refund. The bogus link site was **tax-disc.gov.uk.dvla.mal.pw**, which takes you to an equally bogus **UK Gov** looking site. This site asks for your bank details so they can refund your money direct in to that bank account. The man although capable and astute, only just managed to stop himself pressing *Send* with all his bank details.
Genuine organisations, including the DLVA, will never approach you in this way. Never give personal information to unexpected callers. If you or someone you know has received such a text, and are at all vulnerable, please report it.

If you or someone you know is vulnerable and has been a victim of fraud call Sussex Police on 101 or visit www.sussex.police.uk

OPERATION SIGNATURE
Protecting vulnerable victims of fraud

If you need to a report fraud or attempted fraud, you can do so by contacting Action Fraud at or by calling 0300 123 2040. You can also read the latest Action Fraud alerts at www.actionfraud.police.uk/news or by following @actionfrauduk on Twitter.