Wealden District Neighbourhood Police Team Community Newsletter

- Scam Focus -

Scam police and bank callers

Residents receive phone calls from people claiming to be from the police or their bank.

The caller says they are investigating fraudulent activity on people's accounts. They request people's help in investigating the fraud and ask people to disclose their bank details, such as account and PIN numbers.

Correctly, the majority of people identify this as a scam and refuse to part with their personal and bank details. However, unfortunately some have fallen victim to this scam and subsequently had thousands of pounds stolen from their account.

Whilst arrests and convictions are continuing to be made, offenders are still targeting vulnerable and older people - the majority of people targeted are aged over 60. It is therefore vital that these people in particular are aware of the scam, so please share this information with your neighbours and relatives.

How does the scam work?

The offender calls the victim, purporting to be a police officer, and tells them they are investigating a fraud on their bank account and have someone arrested. They might also claim to be from the victim's bank, again stating they are investigating fraudulent activity on their account.

The offender asks for account information, including card, security and PIN numbers. Sometimes the offenders will ask victims to 'key in' their PIN number into the phone – the number is then captured by the offenders.

They may also ask the victim to withdraw a large sum of cash from their bank or building society. If they make this request they will explain that the money is required as it needs to be forensically examined. They also instruct the victim not to tell the bank why they are withdrawing the money, giving the reason that the bank might be involved in the fraud.

The victim is then instructed to put the bank cards and/or money into an envelope and give them to a courier or taxi, which is sent to the house by the offenders to collect the items. If bank cards are collected they will be later used by the offenders to withdraw money.

In some cases the victim might become suspicious and doubt the validity of what the caller is saying. If this happens, the offender will suggest they call the police via 999 or 101 or contact their bank in order that the victim can confirm the caller's identity.

However, what the victim doesn't realise is that the caller hasn't hung up so the line remains open, even if the victim hangs up, so the victim is put straight back through to the offender who will then pretend to be another person. This 'new' person will then validate the original caller's claims.

What should you do if you get a call?

If you receive a call you're not expecting, you should be suspicious. The vital things to remember are that your bank and the police would

• NEVER ask for your bank account details or PIN number over the phone, so do not disclose these to anyone, no matter who they claim to be.

• NEVER ask you to withdraw money and send it to them via a courier, taxi or by any other means.

• NEVER ask you to send your bank cards, or any other personal property, to them via courier, taxi or by any other means.

If you are not happy with a phone call and are suspicious of the conversation you have with the caller then please end the call and report it to us.

Remember, when reporting a suspicious phone call to police, wait at least five minutes before attempting to make the call to ensure you're not reconnected to the offender. Alternatively, use a mobile phone or a neighbour's phone or test your landline by phoning a friend or relative first, to ensure you aren't still unwittingly connected to the offender.

If you have concerns about your bank account, visit your local branch.

How to protect yourself:

Remember to follow the above advice. In addition to this, some phone companies offer call screening services that can be effective in blocking marketing cold calls and bogus callers.

Contact your phone company and ask about call screening and caller display services.

How else can you help? :

Please share this information with your older relatives and friends: this crime has a devastating effect on people and we need to raise awareness to prevent further people becoming victims.

Report any calls you believe are suspicious as we may be able to trace where the calls are originating from. Please remember, to wait at least five minutes before calling police or use a mobile or neighbour's phone.

Report suspicious activity at cash points. If you see someone spending a long time at a cashpoint, using a number of different cards and have a hood up or their faces covered, contact police immediately. Often offenders will use cashpoints in the early hours.

INVESTMENT SCAMS:

Police are warning of investment fraud after a number of victims have lost money to scams.

During the first lockdown, police have recorded 20 cases of investment fraud where the victim is deemed vulnerable, resulting in a total loss of £1,208,864 in Sussex.

The scams typically involve a fraudster pretending to be from an investment company, offering victims opportunities and claiming they're likely to profit from them. The victims then realised they have been scammed and report it to police.

The majority of victims have been contacted by telephone, but some were found on social media and others were looking for investments online.

A woman in her 60s from Sussex received calls from men claiming to be from Blackrock investment company.

She was persuaded by the fraudsters to invest and write a cheque for £75,000 that was collected by courier. This cheque did not go through, so the victim went into her bank and made a transfer of the same sum to an account.

The victim reported to her bank and it is being investigated.

A man in his 70s from Sussex was searching online for where to invest when pop-up came up from what appeared to be an investment company.

He was contacted by a man saying he is from the company and was talked through possible investment opportunities.

The victim said everything seemed very plausible and legitimate due to what he read online and what he was told by the fraudster so decided to go through with it.

He tried to send £25,000 but his bank fortunately stopped it. He then tried to send £10,000, £10,000 and £5,000.

The man sent him a message saying he received £5,000 but nothing else.

The victim got in contact with his bank to find out why and he was passed onto Action Fraud. Thankfully he managed to get all his money back.

PC Bernadette Lawrie, Financial Safeguarding Abuse Officer for Sussex and Surrey Police said: "We are seeing victims lose devastating sums of money to fraudsters and are urging people to be wary when contacted by strangers about their money.

"If you are thinking of making an investment always check people are from where they say they are.

"Take your time to make decisions and remember that if something sounds too good to be true then it probably is."

If you think you have been victim of fraud, always speak to someone, tell your family, or friends, and contact us on 101, or on the Sussex Police website www.sussex.police.uk

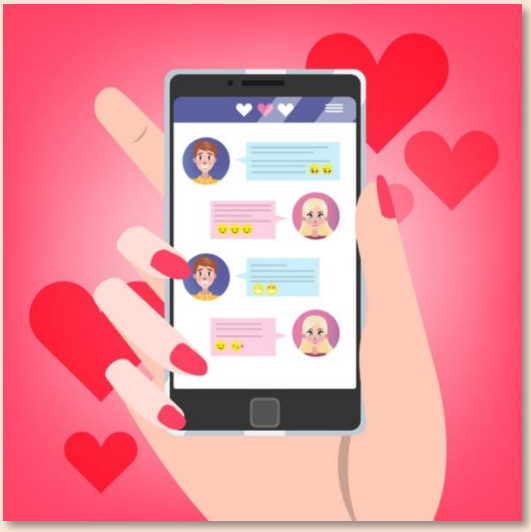
A digital copy of the latest Little Book of Big Scams can be viewed and downloaded: www.sussex.police.uk/SysSiteAssets/media/downloads/sussex/advice/operations-initiatives-and-watch-schemes/operation-signature/the-little-book-of-scams - alternately you can obtain one from your local Police front office or Police contact point.

ROMANCE FRAUD:

Romance fraud targeting lonely and isolated victims during the lockdown is on the rise.

Suspects invest significant amounts of time into socially engineering their victims – knowing that as they gain the victim's trust, their chances of extracting considerable funds from them simultaneously increase.

Fraudsters do not initially ask the victims for money; instead they spend time communicating with them online and building trust. By the time they ask for large sums of money, the reasons for requiring financial assistance have greater plausibility. This is known as the 'grooming period'.



Typically, the longer the period between the date of first contact and the date of the first financial transfer, the higher the amount of money handed over.

Data implies that a high proportion of victims are lonely, widowed or recently bereaved, have suffered from a recent break up and/or suffering from depression.

The financial losses are high and victims can often be in denial, making self-reporting low and repeat victimisation likely.

Romance fraud is one of the fastest growing crime types affecting the vulnerable, so much so that in Sussex all victims of romance fraud are treated as vulnerable by crime type.

Here's how to spot the signs of romance fraud and keep your money safe:

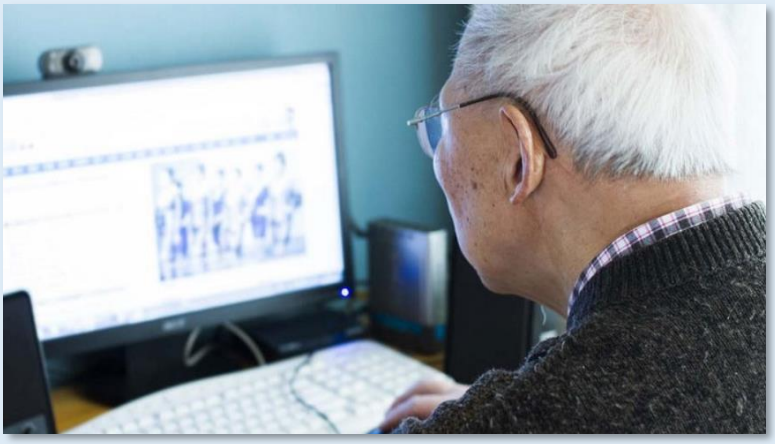
- Be wary of giving out any personal information to someone you don't know. This could be your address, even if it seems to be for a harmless reason such as sending you a gift or flowers
- Never agree to keep your online relationship a secret
- It's a big red flag if someone keeps making excuses not to video chat or meet in person.
- Get to know the person and not the profile
- Never send money or share your bank details on the platform, even if you're told a story which pulls at your heartstrings and seems like a genuine emergency
- Stay on the dating messenger service until confident the person is who they say they are
- Run a search on the internet for their name or any picture they have sent along with the term 'scam'
- No matter how long you've been speaking to someone online and how much you trust them, if you haven't met them in person **do not**:
- send them any money
- allow them access to your bank account
- transfer money on their behalf
- take a loan out for them
- provide copies of your personal documents such as passports or driving licenses
- invest your own money on their behalf or on their advice
- purchase and send the codes on gift cards from Amazon or iTunes
- Agree to receive and/or send parcels on their behalf (laptops, mobile phones etc.)

SOFTWARE SCAMS:

Sussex Police is urging people to be wary of software scams after the Force has received 77 reports from vulnerable victims so far this year with losses totalling £154,454. The average loss has been around £2,000.

The scam typically involves the victim being told they have been hacked or their computer has a virus. They're advised they need to install software, pay money or hand over details to protect their device from further damage.

A 60-year-old woman in Sussex was contacted by a man purporting to be a security technician from Amazon and said her online security was at risk. She was told had been hacked by someone in California and her IP address was not secure. The victim was advised to download an app which then gave scammers access to her computer. They took her financial and personal details and transferred £7,900 from her accounts. The victim realised and contacted police.



Similarly, an 80-year-old man in Sussex received a call saying his computer had viruses and security issues. The victim thought this was odd as he had paid around £600 a few months ago to McAfee for anti-virus and computer protection, which was a three year subscription. The fraudster persuaded the victim to give remote access to the computer and asked him to transfer £900 via Moneygram to sort out the problem. The victim returned to his computer to find that he could not enter is password and had been locked out of it.

"Please be wary if you receive an unsolicited call about the security of your computer. There are fraudsters out there who will try to capitalise on your concern to financially profit.

"We're urging people to be careful make sure you know who you're talking to. Remember - Computer firms do not make unsolicited phone calls to help you fix your computer. Fraudsters make these phone calls to try to steal from you and damage your computer with malware.

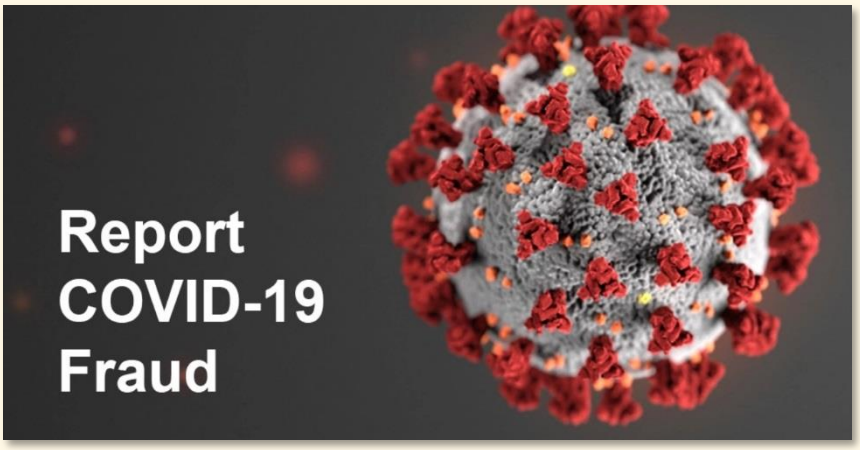
Treat all unsolicited phone calls with scepticism and don’t give out any personal information. If you feel pressured, hang up and talk it through with a friend or family member”.

If you receive an unsolicited call:

- don't allow remote access to your computer
- don’t be rushed or pressured into making a decision - a genuine bank or another trusted organisation won't force you to make a financial transaction on the spot; they would never ask you to transfer money into another account for fraud reasons
- remember to stop and take time to carefully consider your actions
- don't make a payment
- make sure you know who you are talking to - if in doubt, hang up immediately
- listen to your instincts - if something feels wrong then it is usually right to question it
- remember that criminals may lull you into a false sense of security when you are out and about or rely on your defences being down when you’re in the comfort of your own home - they may appear trustworthy, but they may not be who they claim to be

COVID-19 SCAMS:

Police are reminding Sussex residents to stay on the alert as reports come in from elsewhere across the country of frauds or attempts related to the current Covid-19 coronavirus issue.



The majority of reports are related to online shopping scams where people have ordered protective face masks, hand sanitiser and other products, which have never arrived.

Phishing emails is another 'tool' fraudsters have been using during the lockdown period.

These types of emails attempt to trick people into opening malicious attachments which could lead to fraudsters stealing people's personal information, email logins and passwords, and banking details.

Some of the tactics being used in phishing emails include:

• Fraudsters purporting to be from a research group that mimics the Centre for Disease Control and Prevention (CDC) and World Health Organisation (WHO). They claim to provide the victim with a list of active infections in their area, but to access this information the victim needs to either click on a link which redirects them to a credential-stealing page or make a donation of support in the form of a payment into a Bitcoin account

• Fraudsters providing articles about the virus outbreak with a link to a fake company website where victims are encouraged to click to subscribe to a daily newsletter for further updates

• Fraudsters sending investment scheme and trading advice encouraging people to take advantage of the coronavirus downturn

• Fraudsters purporting to be from HMRC offering a tax refund and directing victims to a fake website to harvest their personal and financial details. The emails often display the HMRC logo making it look reasonably genuine and convincing

You can protect yourself from these types of scams by:

- watching 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

- when 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

- protecting your devices from the latest threats - always install the latest software and app updates to protect your devices from the latest threats. The National Cyber security Centre offers advice on looking after your devices.