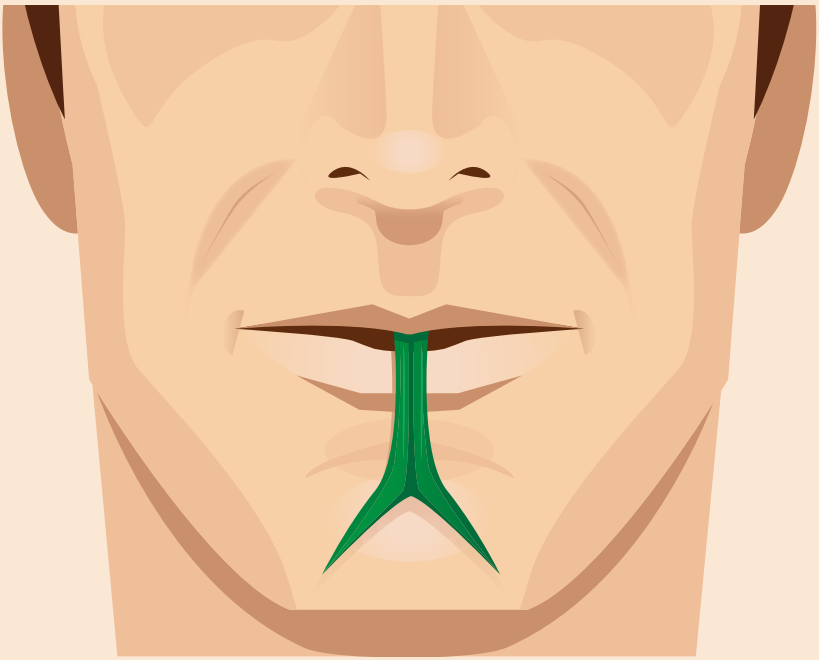
SCAMS BOOKLET



This booklet will identify the different types of scams ongoing in your area.

People aren't always who they say they are, anyone can become a victim of a scam.

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

101 IN AN EMERGENCY ALWAYS CALL 999

Doorstep Crime

Is known to be under-reported, both in terms of attempts and crimes taking place. From bogus callers to rogue traders, doorstep criminals are cunning, creative, and often very convincing. Anyone can be fooled as these people are professional con artists. Generally older people tend to be targeted for various reasons. If you think you could have been a victim or if you have had people unknown coming to your door, please contact 101... It could stop someone else becoming a victim.

Rogue Traders

Will normally cold call, claiming to be workers offering to sell services, make repairs or carry out work on your house, garden or driveway. They will charge inflated prices for zero, sub-standard or unnecessary work. This will involve several tactics including asking for payment upfront and usually via cash or most recently bank transfer. Fraudsters will exaggerate the supposed problem, such as rotten windows, woodworm, loose/broken tiles or offer tree pruning services, clean or replace drive-ways surfaces. They will place a need of urgency to get the work started and pressuring you into making a financial decision there and then or state that they only in the area for a short time. They may also offer OAP discounts or longer guarantees in an attempt to sweeten the deal.

Bogus Callers

Will try to get into your home or obtain personal details by pretending to be someone they're not, including council staff, charity collectors, meter readers and police officers. In reality, they are criminals trying to steal money and valuables. They may have fake identification and will only show it to you quickly (if you ask them). Once access is gained, they will use a distraction technique by asking for you to remain in a room and request you turn on kitchen taps or flush the toilet several times to "check the pressure". Once the fraudster is inside your home, the object will be to steal cash either from bags, purses or large quantities of cash throughout your home without your knowledge. On occasion, whilst you are carrying out their distraction technique you will be unaware of another associate who will assist with the location of your money or jewellery.

Advice

Before undertaking any renovations or work on your home, ask yourself - Do I really need this work done? Speak to friends, family or neighbours to check the work actually needs carried out and if they can advise of a reputable company. Obtain a few quotes from reputable companies and NEVER pay moneys upfront, wait until the work has been completed and you are satisfied with the outcome prior to making any payment.

Be on guard of persons turning up unexpectedly, keep both front and back doors locked and don't keep large sums of cash within your home. Some companies offer a password system. Ask your utility providers if this can be used and if you have a password with a company make sure the caller uses it.

If someone presses your buzzer, rings your bell or chaps your door unannounced, please follow these 3 basic guidelines:

STOP

Always look out your window, buzzer screen or spy hole to see who it is.
DON'T OPEN YOUR DOOR

THINK

Is the caller known to yourself, do they have an appointment?
IF NOT, DON'T LET THEM IN!

CHECK

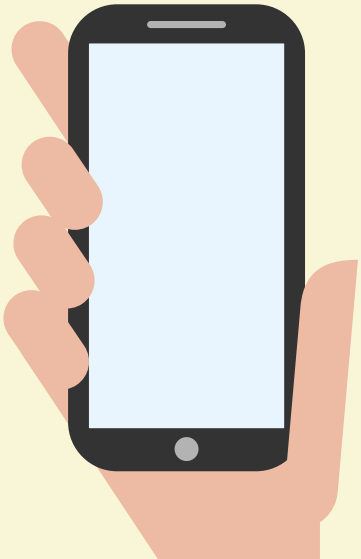
If in doubt, don't open your door, call police for non-emergency on **101** or in an emergency call **999**

Phone Scams

Be wary of unsolicited phone calls from persons saying that they are from your bank, telephone provider or government agency particularly if they are asking for any personal information, passwords, PIN numbers etc. Review your bank and credit statements on a regular basis.

Bank Scams

Fraudsters will contact you pretending to be from your bank and advising that there has been suspicious activity on your account. They will state that you will have to move funds into a "safe account" that they have set up for you. They will ask you to "confirm" your bank details such as your name, address, date of birth, place of birth, PIN number and/or password. Once the funds have been transferred, the safe account will be emptied and your cash will be lost. The bank will not refund you the money if you have provided fraudsters with the PIN/ password.



Fraudsters will also call, providing you with a similar scenario and state that investigations are ongoing with front counter staff and not to tell any bank members, friends/family about this as it may interfere with the investigations. Fraudsters will ask for you to withdraw a large sum of cash to pay for an investigation and collect the monies from your home address. Fraudsters will provide you with answers to the banking protocol questions that bank staff must ask when a person withdraws a large sum of money to ensure you are not a victim of a scam.

It is important that you are honest with bank staff and tell them of your situation as you will not be entitled to any refunds if it is found that you have fallen victim to a scam but have answered the banking protocol questions to their satisfaction.

Gift Card Scam

Fraudsters will contact you via telephone claiming to be from a government agency such as HMRC or DWP. They will inform you that there is an outstanding tax amount to pay and that there is a live arrest warrant in place. However the fraudster will offer for you to clear the outstanding tax by attending your bank and withdrawing cash to purchase particular gift cards to a particular value. You will then be asked to contact the fraudster, provide them with a unique 16 digit security number on the rear of each card. Once they have the code, they have control of the full cash amount from the gift card and you are unable to reclaim the money. No Government agency will ever ask for payment by this means and would never contact you by phone to advise you of this.

Foreign Student Scam

Overseas students may purchase a UK compatible SIM card from their home country whilst studying within the UK. Scammers may call the students via their UK SIM card claiming to be an official officer from their home embassy, having known the students personal details and stating that they are investigating a financial crime to which the student is "involved" in. The student is then asked to cooperate with a "police investigation" via social media video call where they are then asked to provide their bank details in order to return money to rightful owner. All monies are then removed from the students bank account.

Advice

Should you receive a telephone call similar to any of the above, hang up immediately, contact bank, Police or trading standards via a different telephone line or wait around 30 minutes before using the same phone. Fraudsters will leave the line open waiting for you to pick up the phone.

Online Scams

Online Scams, also known as Phishing can involve sending malicious attachments or website links in an effort to infect computers or mobile devices. Criminals send bogus emails that often appear to be authentic communications from legitimate organisations with embedded links that direct you to a hoax website and request your login or personal details. You may also run the risk of your computer or smartphone being infected by viruses. Once your personal details have been accessed, criminals can then record this information and use it to commit a scam such as identity theft and bank fraud.

Bank Scams

You receive an email from what you believe is your bank, addressed to "customer". This email will state that you need to confirm your bank details or your online bank account needs urgent attention. You will note a threat/need of urgency to access your account which states that your account may be closed if action is not taken to rectify the issue(s). A link will be attached in the email, this will take you to an identical login page, however once you have logged in via this email, your account will be hacked and your accounts will be emptied.

Refund Email Scams

Similar to bank scams, you may receive an email from an online payment service, market/auction sites or utility companies stating that you are due a refund by clicking on the link attached in the email. You will be asked to log in or complete personal details that criminals record and use this to commit identify/bank fraud.

Advice

Banks will never contact the customer via email to ask for passwords or sensitive information by clicking on a link and/or visiting a website. Fraudsters are unlikely to know your name, so the email may address you in vague terms, for example 'Dear Valued Customer'. Phishing emails may probably contain spelling or grammatical errors in the email or subject box.

Useful Contacts

Citizen Advice Scotland
03444 111 444
www.cas.org.uk

Glasgow City Council
Trading Standards
08081 646 000
www.glasgow.gov.uk

East Renfrewshire Council
Trading Standards
0141 577 3001
www.eastrenfrewshire.gov.uk

East Dunbartonshire Council
Trading Standards
0300 123 4510
www.eastdunbarton.gov.uk

Police Scotland
101 – Non Emergency
999 - Emergency
www.scotland.police.uk

Age Scotland
0333 32 32 400
www.ageuk.org.uk/scotland

Neighbourhood Watch Scotland
www.neighbourhoodwatchscotland.co.uk

Scottish Fire and Rescue Service
0141 887 1188 - Non Emergency
999 - Emergency
www.firescotland.gov.uk