Community Council Report

This report covers progress we have made in dealing with your priorities for the Kincardine and Mearns Community Council area for the period May 2025.

The report aims to highlight emerging issues in your area, provide crime prevention advice and guidance to Community Council members and the residents you represent. Our focus is to reduce crime and disorder, help create safer communities and respond effectively to local concerns.

In this report I will focus on Police Station 'areas' as historically these stations would covers the following areas.

Portlethen and surrounding areas including Drumoak and Durris. I will specify this as Portlethen.

Stonehaven Police Station – Stonehaven, Newtonhill, Drumlithie and surrounding areas. I will specify this as Stonehaven.

Laurencekirk Police Station – Laurencekirk and surrounding areas including Fettercairn, Edzell woods, Auchenblae and Garvock. I will specify this as Laurencekirk.

The A92 towns (Catterline – St Cyrus) along the coastal Road are covered between Stonehaven and Laurencekirk but I will specify them as Coastal Road.

Community Policing Priorities

Antisocial behaviour, Violence and Disorder:

Area	Youth Disorder	Anti-Social
Portlethen	20	10
Stonehaven	16	18
Laurencekirk	1	2
Coastal Road	4	3

Acquisitive Crime: D – Detected UI-Under Investigation

Area	Thefts	Shopliftings	Theft of motor vehicle	Housebreakings/Attempts
Portlethen	0	2D,1UI	1D	1D, 1UI
Stonehaven	0	6D,2UI	0	0
Laurencekirk	0	1D	1UI	1UI
Coastal Road	0	3D	0	1D,1UI

Road Safety & road crime:

Area	Careless Driving	Drink/Drug Driving	Dangerous
Portlethen	5D	3D,1UI	1D
Stonehaven	3D	1D	0
Laurencekirk	1D	0	0
Coastal Road	0	0	0

Community Engagement & Reassurance:

As a community we are continuing to see members of the public be caught out so please make use or share the below with family, friends and neighbours.

Cyber-fraud is the most common and changing form of financial crime affecting Scotland.
The use of technology to target both people and organisations has become more common. This can be from simple scam emails to cyber-attacks and social engineering techniques which is used to extort large sums of money from victims.

Phishing

Warning signs:

- E-mail that uses generic terms like ‘Dear account holder’
- E-mail is threatening and states that urgent action is required
- E-mail has a link you don't recognise
- Spelling errors in the e-mail
- E-mail address is different from trusted company’s website
- Unexpected e-mails from a company you have no business with
- No padlock sign on website and no 'https://' at the beginning of web address.

Keep yourself safe:

- Keep your browser software up-to-date
- Avoid risky sites, including supposed investment sites
- Never click on a link in an e-mail from an unknown person
- Use spam filters if you can
- Never give out your personal details, passwords or security codes via e-mail
- Don’t leave personal documents lying around for anyone else to see
- If you're throwing away correspondence, remember to shred it first.

Fraudulent transactions and identity fraud

Purchases made without the person's consent is one of the most reported forms of cyber-enabled fraud.
This is when a fraudster gets access to their victim's accounts or uses their payment details to take money or buy things.
These offences use different phishing techniques to get a victim’s account details. The fraudster also uses the victim’s debit/credit card or phone. They then use these to carry out transactions online.

Access can also be gained through remote access to a victim's devices. The fraudster then gets access to their accounts.
If any transactions on your account are suspicious, contact your bank/credit card company as soon as possible. You should report this and allow them to carry out an investigation.

Online shopping/action frauds

Fraudulent sales and purchases is one of the most common forms of cyber-fraud. Fraudster either advertise products that do not exist or agree to buy items and then not paying for them. This is done on sites such as eBay, Gumtree, Depop and Schpock.
The most common items in these scams are electronics and vehicles. Tickets are also advertised at prices below regular market prices.
When making fake purchases, fraudsters will send fake confirmations of payment to the victim of the scam. This could be a fake PayPal email.

Internet auction sites

Internet auction and private selling sites can be very useful for the public.
However, they are also the targets of fraudsters. Several thousand would-be traders fall victim every year.
These sites assist in transactions between sellers and buyers. Sellers post items for sale with terms and conditions set. Potential buyers then make ‘bids’. The person who makes the highest offer in the time wins.
Arrangements are then made for the payment and delivery of the goods.
Payment is often arranged through an escrow service. These services hold the buyer’s payment until the goods have been received and checked.
The buyer then allows the escrow service to pay the seller.

Invisible goods fraud

The buyer sends the payment, but no goods are delivered. The seller cannot be contacted as false details were given.
Using a legitimate escrow service can help protect the buyer from this type of fraud.

Non-payment fraud

This can happen where the seller agrees to payment after delivery.
It can also occur if a stolen credit card is used to make payment to an escrow service. This is then not discovered until after the goods are sent.
However, this is different from the case where there is no payment made due to a dispute between buyer and seller.

Online escrow fraud

Fraudsters have created genuine looking websites which offer escrow services. This is done to defraud customers.
The seller follows instructions on how to pay their money to the escrow site. This is usually done through a cash transfer system, such as Western Union.

The escrow site then fails to pass the money on to the seller. They then can no longer be contacted by either party.
Fraudsters also use a number of other methods to get as much money as they can. Escrow fraudsters can commit invisible goods frauds. They can also contact the losing bidders for genuine auctions, claiming to be the seller with a similar product for sale.
In both cases, the fraudster insists that payment is made through their fraudulent escrow service.
Escrow fraudsters can make sure winning bids on genuine auctions for high-value goods. Again they insist that payment is made through them.
When the seller checks the escrow service, they sees that the payment has been made by the buyer. They then send off the goods (usually to a foreign address).
The seller then loses contact with the buyer and the escrow service. They then do not receive the promised payment.

Courier scams

Fraudsters also get victims who are selling items online, to make payments for couriers which do not exist.
The fraudster will express interest in buying, but request that delivery be made by a courier they trust. They will then request the victim make the payment to the courier. They may claim to have sent payment for both the item being sold and the courier, alongside a fake payment confirmation. They then request that the victim pay the courier using this money.
Payments of the courier are then paid into an account owned by the fraudster. Contact will then stop.
There are a number of steps that can be taken to minimise the risks of carrying out business on the internet:

- Get to know the auction site's terms and conditions.
- Get to know the seller/buyer
- Check the auction website for feedback on this person
- Find out details, such as a permanent address and landline telephone number
- Carry out online checks to verify that information
- Ask questions about the goods
- Try to verify that a seller has the items in front of them
- Consider the payment arrangements requested
- Fraudsters will often insist on high-risk payment methods such as cash, cheque, wire transfer or cash transfer systems such as Western Union or Nocheques
- Consider the seller/buyer's location
- Very few internet auction frauds occur with the buyer and seller in the same police force area. Although these fraudsters do operate within the UK, they prefer to commit their frauds in foreign countries. This is because international crime investigation can be difficult
- Check out escrow services - especially if the person insists on using a particular service
- These sites are often well presented and look genuine. However, these fraudulent sites may have a number of spelling and grammar mistakes.

If you do find yourself a victim of internet auction fraud, report the fraudulent transaction to the internet auction site itself. You should then contact your local police office.

Impersonation scams

Fraudsters can hack social media and email accounts. This is done to impersonate trusted friends and family.
Fraudsters will gain control of accounts, predominantly Facebook, and message the account's contacts asking for money.
If you are contacted by someone claiming to be a friend or family member through a social media site, contact them using something else, i.e. by telephone, before agreeing to give them money.

Romance fraud

Through romance fraud, fraudsters can get large amounts of money from victims over a long period of time.
Contact with victims is usually made through dating apps. The fraudsters then get into a relationship with the victim.
They will pretend to be someone living or working overseas. They will then request money from the victim to pay for flights to the UK to visit the victim, medical bills or legal issues.
These requests will often be repeated over a long period until the victim realises it is a scam.

Technical support scams

This is where victims are called from someone pretending to be from some sort of technical support. This could be a representative from their Internet Service Provider or Microsoft.
They may also have a pop-up message appear while looking through internet. It will claim there is an issue with their PC and that they must contact a number to fix it.
Fraudsters will claim there is a fault with the device or internet (slow internet speeds, malware, system updates). In order to fix the problem, the victim must allow them access to their device. This is done by installing various programs.
The fraudster then gets access to the device. They then get access to the victim's banking accounts or get them to make payments for fake services.
They then install malware on the device such as spyware and are able to get further details from the victim.

Investment scams

Investment scams are the most profitable form of cybercrime affecting Scotland.
These scams get victims to make payments with a promise of unrealistic returns on investments. They will then have to make further payments towards fees and taxes.
A large number of these scams use cryptocurrencies. They will get the victims to invest in new cryptocurrencies or to buy bitcoin. There will be a promise that it will increase in value.

Blackmail scams

The most common form of blackmail scam is when the criminal sends an email claiming they have filmed the victim looking at pornographic material online.
They say that they will release the video if the victim does not pay them money.
These threats are false. You should not respond to any of these threatening emails.

Business email compromise

Business email compromise is one of the biggest frauds in Scotland and throughout the world.
These frauds can have a devastating impact on victims. They threaten businesses and can take many forms.
Invoice Fraud is where fraudsters use a compromised business email account to send a doctored invoice for services. They request that the payment is sent to an email account controlled by them.
Wage diversion is where fraudsters use an employee's compromised email to contact a company's HR or finance department. They request a change of bank details so they can take that person's wage payments.
CEO fraud is where fraudsters pretend to be the CEO or a high ranking executive in a company. They request that an employee pays them money.
Solicitor/accountant – Fraudsters can also pretend to be a solicitor or accountant and get their clients to transfer money to them.
Individuals and organisations should make every effort to protect themselves by keeping their firewalls/internet security up to date.

Cryptocurrency

Cryptocurrency related investment scams continue to be prevelant across various social media platforms, which can result in significant financial loss (i.e. lifesavings, pension etc.) and in some cases may lead to increased risk of causing mental health issues such as depression and anxiety.
During lockdown cases of cryptocurrency investment scams increased. It is believed that the number of victims falling for this may be significantly higher as it is suspected many cases go unreported to Police.
The best way to protect victims is to encourage them to be careful and selective about the websites they visit and whom you engage with online, especially when considering to invest large amounts of money - Cryptoassets | FCA
Below are some details of the potential signs of this type of crime, along with advice and support that is available to those who may have been affected.

What is Cryptocurrency?

Cryptocurrencies are digital currencies that are known for their market volatility so the value of investor's assets go up and down quickly. Criminals can take advantage of the unregulated nature of cryptocurrencies to scam consumers. Cryptocurrency can be traded or exchanged online to buy from people or companies who accept this form of payment.

Cryptocurrency investments are often made via currency exchange platforms. These are websites where you can buy, sell or exchange cryptocurrencies for other digital currency or traditional currency like GBP or US dollars.
Criminals benefit from the volatility of the cryptocurrency markets, pressuring people to make decisions without due diligence or consideration.
Some people who have been scammed don't realise for some time. They may make multiple or regular payments to the criminal and only realise when they try to withdraw their money from the 'scheme'.
If something goes wrong with a cryptocurrency investment you are unlikely to get your money back, because they mostly aren't covered by the UK's Financial Services Compensation Scheme.

The National Cyber Security Centre (NCSC) published figures which showed that as of March 2022, 11 million phishing scams were reported which resulted in 78,000 scams being removed – Fake cryptocurrency investment lures make up more than half of all online scams detected.

Who is behind this crime?

This type of crime can be carried out by lone individuals or organised crime groups who are maybe based overseas. For perpetrators it's a low risk way to make money, and they can reach a wide range of individuals easily online. The perpetrator(s) is gambling that enough people will respond so that their scam is profitable.

Examples of Cryptocurrency

Scams Celebrity Endorsements

Arun saw a 'celebrity endorsed' social media post advertising the promise of big returns on Bitcoin. He contacted the company and following a phone call with a "trader' was convinced to make a payment of £300. After logging into his trading account on the website, he saw his investment increase. Arun continued to invest more money following pressure from another "trader" from the company and was persuaded to take out a loan sourced by the criminal. Arun only realised it was a scam when he was unable to access his account to withdraw his money or contact the company.

Mining scheme scam

Emma had owned cryptocurrency for a few years and the value of her investment had gone up and down. Some of Emma's friends got into crypto mining, and they said it was a great opportunity to make passive income on the side, without much effort or knowledge. Having joined a mining group on social media to find out more, Emma was contacted by a 'successful cryptocurrency trader' who offered her fixed returns for an investment in a mining programme. Emma transferred some of her cryptocurrency to the trader, but she realised she had fallen for a scam when the trader became uncontactable.

New coin scam

Jadon had heard loads about cryptocurrency traders putting money into Bitcoin years ago and making a fortune. The influencers he followed on social media encouraged everyone to get involved. He went online to do some research and concluded he needed to invest in a new coin to make the most money. Jadon saw an advert for a new coin and found it on a brokerage site. The advert said he could triple his money in months and that the makers of the coin had an office in London. Jadon put most of his savings into the coin as he wanted to maximise his returns, and he was told he wouldn't loose anything as he was buying in at the start. It only dawned on Jadon that he had been a victim of a scam when his account stopped working and he was asked to make another payment to access his funds.

How to spot a Cryptocurrency Scam?

- You see adverts on social media, sometimes celebrity endorsed, offering unrealistic returns on investments
- You're contacted by phone, email or social media about an opportunity using aggressive techniques and incentives to buy before certain deadlines
- You're told your buying in at the perfect time. You may be offered a high return on your investment with apparently little or no risk
- You're pressurised into making a decision with no time for consideration
- You're told the investment opportunity is exclusive to you
-

How to protect yourself?

- Don't assume it's real – Professional-looking websites, adverts or social media posts don't always mean that an investment opportunity is genuine. Criminals can use the names of well-known brands or individuals to make their scams appear legitimate.
- Don't be rushed or pressured into making a decision – A genuine bank or financial organisation won't force you to part with your money on the spot. Always be wary if you're pressured to invest quickly or promised returns that sound too good to be true.
- Stay in control – Avoid uninvited investment offers, especially those over cold calls. If you're thinking about making an investment, get independent advice and thoroughly research the company first.
-

Advice for victims of investment scams

If you or someone you know has been a victim of an investment scam, don't feel embarrassed, help and support is available.

1. Contact the Police immediately. The police will take your case seriously, will deal with it in confidence.
2. Contact your Bank immediately. Ensure all pending/future transactions are cancelled.
3. Report to Financial Conduct Authority (FCA). Phone their Consumer Helpline on 0800 111 6768 or using their report form.
4. Don't communicate further with the criminals. Take screen shots of all your communication. If they contacted you via Social Media, suspend your account (but don't delete it) and use the online reporting process to report the matter to Instagram, Facebook etc. Deactivating your account temporarily rather than

shutting it down will mean the data are preserved and will help police to collect evidence. Also, keep an eye on all the accounts which you might have linked in case the criminals try to contact you via one of those. If you were contacted by email, you can forward the email to the NCSC's Suspicious Email Reporting Service (SERS) on report@phishing.gov.uk, and then delete it.

5. Preserve evidence. Make a note of all details provided by the offenders, for example; the email address, number or social media account that you have been contacted from; the Western Union or MoneyGram Money Transfer Control Number (MTCN); any bank account details; cryptocurrency wallet, etc.
6. Block and report. Report them to the platform they have contacted you on and block the individual on the platform / in your contacts.
7. Don't panic. It can be a very distressing situation for some people but there is lots of help, advice and guidance out there.

DO NOT DELETE ANY CORRESPONDANCE

How to secure your cryptocurrency wallet

Be careful with online services – Exercise caution when considering online services for storing your funds. Many exchanges and online wallets have suffered from security breaches in the past and such services generally still do not provide enough insurance and security to be used to store money like a bank. Therefore, it may be prudent to explore alternative Bitcoin wallet options. Should you opt for such services, select them with meticulous care. Furthermore, employing two-factor authentication is strongly advised.

Small amounts for everyday uses – A bitcoin wallet is like a wallet with cash. Just as you wouldn't carry a large sum in your pocket, it's wise to apply the same principal to your Bitcoin wallet. Typically, it's advisable to store modest amounts in your computer, mobile, or server for everyday transactions, while securing the majority of your funds in a more secure environment
Backup your wallet – Stored in a safe place, a backup of your wallet can protect you against computer failures, human errors, and theft of your mobile or computer. To safeguard your wallet:

- Backup Completely: Some wallets contain hidden private keys. Ensure your backup includes all private keys to recover your full funds.
- Encrypt Online Backups: Online backups are susceptible to theft. Protect your data with encryption, especially when exposed to the network.
- Diverse Storage: Avoid single points of failure by storing backups in multiple secure locations, such as USB keys, paper and CD's.
- Regular Backups: To include recent Bitcoin addresses and changes, perform regular backups.
-

Encrypt your wallet

Encrypting your wallet or your smartphone allows you to set a password for anyone trying to withdraw any funds. This helps protect against thieves, though it cannot protect against keylogging hardware or software:

- Remember your password: Losing your password means losing your funds. Bitcoin offers limited recovery options, so store it securely, even for extended periods. A paper copy in a secure location is a wise precaution.
- Strong password: Avoid using predictable passwords (such as dates, family and pet names). Avoid the most common passwords that criminals can easily guess (like 'passw0rd'). To create a memorable password that's also hard for someone else to guess, you can combine three random words to create a single password (for example cupfishbiro).

Offline wallet for savings

An offline wallet, also known as cold storage, provides the highest level of security for savings. It involves storing a wallet in a secured place that is not connected to the network. When done properly, it can offer a very good protection against computer vulnerabilities. Using an offline wallet in conjunction with backups and encryption is also a good practice. Here is an overview of some approaches:

- Hardware Wallets: Strike a balance between high security and ease of use with hardware wallets. These dedicated devices offer robust protection against computer vulnerabilities and online threats. They are incapable of installing additional software and backup options ensure recovery in case of devices loss.
- Offline transaction sigining: Employ two computers, one offline with the complete wallet and transaction-sigining capability, and one online with a watching wallet for unsigned transactions. This enables secure transaction issuance
- Create a new transaction on the online computer and save it to a USB key
- Sign the transaction with the offline computer
- Send the signed transaction using the online computer. In the event of network compromise, the online computer cannot withdraw funds
-

Keep your software up to date

Ensuring your Bitcoin software is up to date is pivotal. The latest version provides critical stability and security enhancements, preventing a range of issues and introducing valuable features, all while bolstering your wallets security. Equally vital is updating all other software on your computer or mobile to foster a secure wallet environment.

Multi-signature to protect against theft

Bitcoin offers a multi-signature capability, requiring several independent approvals for a transaction to be executed. It’s valuable for organisations, granting access to treasury funds only when, for example, 3 out of 5 members authorise the withdrawl. Certain web wallets also offer multi-signature functionality, empowering users to maintain control over their assets and preventing theft by protecting against the compromise of a single device or server.

Further help and support

If this has happened to you or someone you know please talk to a family member, friend, colleague or line-manager that you trust. Please check out our useful links section with more support channels available along with guidance and links to trusted partner agencies.

Links
Support and Wellbeing:

- Home | SAMH

Further information, advice and guidance:

- Report a scam email - NCSC.GOV.UK
- Report a scam website - NCSC.GOV.UK
- Report a scam advert - NCSC.GOV.UK
- Report a scam to us | FCA
- Financial Conduct Authority | FCA
- Victim Support Scotland