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 February 2024.

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 Policing Station 'areas' as historically these stations would cover the following areas.

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

Stonehaven Police Station – Stonehaven, Newtonhill 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	7	6
Stonehaven	3	16
Laurencekirk	1	8
Coastal Road	0	12

Acquisitive Crime: D – Detected UI-Under Investigation

Area	Thefts	Shopliftings	Theft of motor vehicle	Housebreakings/Attempts
Portlethen	1D	0	0	
Stonehaven	2 UI	0	0	4 UI, 1 D
Laurencekirk	2 UI	4 UI	0	
Coastal Road	1 UI	1 UI	0	

Road Safety & road crime:

Area	**Drink/Drug Driving**	**Dangerous**	**Careless Driving**
Portlethen	0	1 UI, 1 D	2 D
Stonehaven	2 UI	0	0
Laurencekirk	1 UI	0	0
Coastal Road	0	0	0

Community Engagement & Reassurance:

This month I want to go over online safety and February's topic is Online Shopping

Online shopping

Using the internet to buy goods or services is now so easy. Many of us are spending more time shopping online than before.

Unfortunately, fraudsters use online shopping scams. They can hide their identity and target many victims at the same time.

Your online transactions can be targeted by criminals and fraudsters. This is because you cannot see who you are paying money to.

The following tips will help you enjoy a secure online shopping experience.

- Choose carefully where you shop
- Use a credit card for online payments
- Only provide enough details to complete your purchase
- Check your bank and credit card statements regularly
- Check the correct amount has been debited
- Query any suspicious payments with your bank or credit card provider immediately
- Keep your accounts secure
- Watch out for suspicious emails, calls and text messages.

Choose carefully where you shop

Make sure the website you're buying from is genuine. Make sure it's not a fake or copycat site.

Do this by typing in the address yourself. Check the spelling. Web addresses of fake websites are different to real ones. There may be one or two incorrect letters.

Research sellers' and other bidders' selling history and bear in mind that a website ending '.co.uk' doesn't necessarily mean it's based in the UK. Check the address of the company and the phone number.

It's worth doing some research on online retailers to check they're legitimate. Check the seller or buyer's review history. Check feedback from other reviewers.

Beware of accounts that may have been set up very recently. Be careful if the feedback is all positive and sounds similar. This could mean fake reviews.

Read feedback from people or organisations that you trust. Look at consumer websites.

Some of the emails or texts you receive about amazing offers may have links to fake websites.

If you're unsure, don't use the link. Either:

- type a website address that you trust directly into the address bar
- search for it and follow the search results.

Use a credit card for online payments

Use a credit card when shopping online. Most major credit card providers protect online purchases.

Using a credit card (rather than a debit card) means if your payment details are stolen, your main bank account won't be directly affected.

If you paid using a debit card you might be able to make a claim for a refund. This is a voluntary scheme called 'chargeback'.

You should also consider using an online payment platform. These include PayPal, Apple Pay or Google Pay. Using them means the retailer doesn't see your payment details.

There's also a dispute resolution should things go wrong. However, they may not provide the same protection as a card provider. Check their terms and conditions before your sign up.

When it's time to pay, check there's a 'closed padlock' icon in the browser's address bar.

The padlock icon doesn’t guarantee that the retailer itself is legitimate/reputable (and that their website is secure). It means that the connection is secure.

If the padlock icon is not there then don’t use the site. Don't enter any personal or payment details, or create an account. Also be aware if the browser says not secure.

Only provide enough details to complete your purchase

You should only fill in the mandatory details on a website when making a purchase. These are marked with an asterisk (*). They will include your delivery address and payment details.

You shouldn't have to provide security details (such as your mother's maiden name, or the name of your first pet) to complete your purchase.

If possible, don't create an account for the online store when making your payment.

You can complete your purchase without having to create an account. You can use an online payment platform.

If you think you'll become a regular customer with the store, then you may want to create an account.

The store may also ask if they can save your payment details for a quicker check-out next time. Unless you're going to use the site a lot, don't allow this.

Keep your accounts secure

If you're using the same password for your online accounts then you're at risk. You're also at risk if you use a password which is easy to guess.

Hackers could steal your password and then use it to access your other accounts.

For this reason, you should make sure that your really important accounts are protected by strong passwords. Make sure you don't use them anywhere else.

These include your email account, social media accounts, banking accounts, shopping accounts and payment accounts.

This NCSC infographic explains how you can create strong passwords and store them safely. It means you don't need to remember them.

You can protect your important accounts from being hacked by turning on two-factor authentication (2FA). It's also referred to as two-step verification or multi-factor authentication.

Turning on 2FA stops hackers from accessing your accounts. They won't be able to get in even if they know your password.

It does this by asking you to confirm that it's really you in a second way. This is usually done by asking you to enter a code that's sent to your phone.

Watch out for suspicious emails, calls and text messages

You'll probably receive many messages from online stores. You'll get this as a result of 'opting in' to receive messages from them.

Lurking in these genuine messages, may be fake ones. These can contain links which can steal your money and personal details. They can be very difficult to spot.

Of course, not all messages are bad. If something doesn't feel right, follow the NCSC guidance on dealing with suspicious emails, phone calls and text messages.

If you have received an email which you're not quite sure about, forward it to the NCSC Suspicious Email Reporting Service (SERS). Send it to report@phishing.gov.uk.

If you've received a suspicious text message, forward it to 7726. It won't cost you anything. It allows your provider to investigate the text and take action (if found to be a scam).

If you come across an advert online that you think might be a scam report it via, Advertising Standards Authority (ASA) website. This allows ASA to give online service providers with the details they need to remove these from websites.

If things go wrong

If you think your credit or debit card has been used by someone else, let your bank know straight away. They can block anyone using it.

Always contact your bank using the official website or phone number. Don't use the links or contact details in the message you have been sent or given over the phone.

If you think you have responded to a suspicious email or text message, or visited a scam website, read the NCSC's guidance on dealing with scam emails, phone calls and text messages.

All reports of fraud and any other financial crime should be reported to Police Scotland on 101.

Inspector Rhona Di Meola
Kincardine and Mearns Community Policing Team
06/03/2024