Causeway Coast & Glens Policing & Community Safety Partnership

NEIGHBOURHOOD WATCH NEWSLETTER: Edition 21 – Autumn/Winter 2021

REMEMBER TO 'CLOSE IT, LOCK IT, CHECK IT' THIS WINTER

Police in Causeway Coast and Glens are appealing for residents to be vigilant around home security as we come into the winter period.

Chief Inspector Rory Bradley explains: "Now is the time to review your home security, identify any gaps and then put in place measures to stay protected.

"There are a number of initiatives which are really helpful in terms of home security including the 'No Cold Calling' and 'Nominated Neighbour' scheme as well as the Policing and Community Safety Partnership initiative Neighbourhood Watch. You can find out more about these on the police website or telephone 101 and ask to speak to your Neighbourhood Team or our Crime Prevention Officer.

"We are also asking residents to check in on older people you know who are vulnerable or live alone. It can be reassuring for them to know they have a neighbour to call on if they are concerned. There are also steps you can take as a householder to stay safe including keeping doors and windows closed and locked, installing a door chain, and making use of the Quick Check service on 101 should someone call to your door.

"Your call will be answered personally and promptly by a trained police call handler who will check to make sure the person at the door is a genuine representative of the company they are claiming to be from. If they are not or they think that there is something suspicious, the operator will be able send the police to you.

"Please continue to report any suspicious activity to us and be assured that officers are on patrol throughout the District, day and night, to help keep our communities safe."

MESSAGE FROM PCSP CHAIRPERSON COUNCILLOR DARRYL WILSON

I am delighted to have taken over the helm of Chairperson as the Causeway Coast and Glens Policing and Community Safety Partnership (PCSP) and welcome you to the 21st edition of the Causeway Coast and Glens Neighbourhood Watch newsletter.

I have been an active member of the PCSP for several years and have seen the commitment of PCSP members, statutory and community organisations to keep Causeway Coast and Glens a safe and secure area. The last 18 months have been extremely challenging for everyone in society. As we slowly emerge from the difficulties COVID has, and continues to present, it would be remiss of us not to acknowledge that feelings of individual confidence and safety have been affected. With this in mind, we wish to remind everyone of their strength and ability to work together to continue to foster community spirit and deal with concerns collectively in ways that would never be possible individually.

Neighbourhood watch does exactly that, the drive comes from the community itself who take a stand in supporting one another's right to feel safe and provides a voice and support to the most vulnerable in our communities. With the support of PSNI and PCSP we know that the neighbourhood watch network have worked hard to prevent residents from falling victim to crime and combating fear of crime locally and we thank all our neighbourhood watch coordinators for their continued commitment.

I am urging everyone to take time to read the contents of this newsletter for advice on staying safe, please share this information and details of support available, check in on vulnerable family members and neighbours and report any suspicious activities to PSNI.

Members of the PCSP are available to discuss any community safety or policing concerns you may have. There will also be a series of meetings where the public can have their say on policing. These meetings will be organised locally and you can email pcsp@causewaycoastandglens.gov.uk for more details. Prevention is key as we don't wish anyone to be intimidated by or fall victim to anti-social or criminal behaviours.

Why not start the conversations with neighbours about starting a neighbourhood watch scheme in your area? PSNI and PCSP staff will support you through the application process and you can register your interest or get more information on neighbourhood watch by emailing: pcsp@causewaycoastandglens.gov.uk.

Best Wishes and Stay Safe!

Cllr Darryl Wilson

STAY SAFE ON THE ROADS

Already too many people have lost their lives on the roads here in Causeway Coast and Glens and Inspector Davy Burns is taking this opportunity to ask people to take responsibility for ensuring we can all travel safely.

"Far too many people are taking dangerous and completely unnecessary risks, putting themselves and other completely innocent road users at risk," explains Inspector Burns.

"The driving offences our officers continue to detect have the potential to cause the most serious collisions and we will continue to robustly enforce the law to make our roads safer.

"I am asking everyone to take a moment to reset their attitude to road safety. Drivers and riders must slow down, pay greater attention to their surroundings, never drive or ride a motorbike after drinking or taking drugs and whether you are a driver or passenger, always wear a seatbelt.

"Pedestrians and cyclists also need to be aware of their surroundings and, particularly at this time of year, make every effort to be seen by wearing reflective or hi-vis clothing."

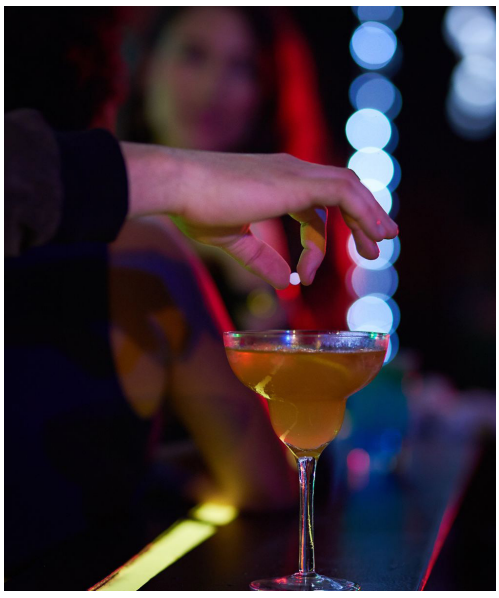
POLICE ISSUE ADVICE FOLLOWING DRINK SPIKING CONCERNS

Police in Causeway Coast and Glens are seeking to improve safety and raise awareness following recent reports of suspected drink spiking in the District and across Northern Ireland.

District Commander Superintendent Ian Magee says: "We take reports of this nature incredibly seriously and anyone found to have carried out such a premeditated and dangerous act could face a potential sentence of up to 10 years in prison.

"We are working closely with bars and clubs across the District to make them as safe as possible. CCTV is in operation in many venues and high streets and is one of our lines of enquiry in terms of identifying perpetrators. If you believe you have been the victim of drink spiking, seek medical advice immediately and make a report to police by contacting 101 or 999 in an emergency."

Information on symptoms to look out for, along with advice on how to help someone who may have been spiked can be found at www.drugsandalcoholni.info



COMMON CYBER THREATS

SOCIAL ENGINEERING
Attackers attempt to trick you into doing 'the wrong thing', such as clicking a bad link that will download malware or direct you to a malicious website.

MALWARE
Malicious software or file that can infect a device and be a security risk to the user.

RANSOMWARE
Locks the user out of their files or their device, then demands an anonymous online payment to restore access.

SPYWARE
Unwanted software that infiltrates your device, stealing your Internet usage data and sensitive information.

MALICIOUS WEBSITES & APPS
Websites or Apps that contain malware or malicious content that compromise your data and device.

UNSECURED WI-FI
Hackers can steal unencrypted data from users' devices accessing the Internet through unsecured public Wi-Fi.

DEVICE THEFT
Criminals steal your device, then use it to commit criminal acts online.

CYBER CRIMINALS WILL LOOK FOR WEAK POINTS IN YOUR HOME TO GET THEIR HANDS ON FINANCES OR SENSITIVE DATA THAT THEY CAN USE FOR THEIR OWN GAIN.

This diagram highlights key weaknesses in the home that you should be aware of.

We have included practical tips (found overleaf) that you can refer to, to help you secure these weaknesses and further guidance can be found on our 'Secure Your Home Information Hub' on our website.

www.nicybersecuritycentre.gov.uk/home-security

ROUTER – YOUR GATEWAY TO THE INTERNET
Your broadband router is the gateway to the Internet and your first line of defence from cyber criminals being able to access your home network or other devices. Learn how to use its security features such as turning on a built in firewall and changing the default login password.

SEE TIPS 2 3 4 5

WI-FI
Don't make your Wi-Fi network on your broadband router easy for cyber criminals to access. All the data that transmits wirelessly around your home needs to be protected. Learn how to secure it correctly and change the default password.

SEE TIPS 3 5

TVS AND GAMES CONSOLES
Most TVs and games consoles can connect to the Internet, which makes them vulnerable to cyber security breaches if they're not securely set up and kept up to date by enabling automatic software updates.

SEE TIPS 8 10 11

COMPUTERS & LAPTOPS
These devices hold and process a lot of your personal data. It is important to properly protect them from unauthorised use and from viruses (also called malware). Learn the basics of securing your devices and be sure to install anti-virus software.

SEE TIPS 1 4 5 6 7

SMART PHONES & TABLETS
Mobile devices carry as much data as a PC or laptop. Because they are portable, they can be easily lost or stolen. Learn how to secure them correctly.

SEE TIPS 1 5 6 8 9 10

HOME OFFICE
When working from home it's important to keep your devices secure against cyber criminals and unauthorised access by family and friends. Portable devices can be lost or stolen more easily, which means the data on them could be at risk. Make sure you know how to report any problems to your IT department.

SEE TIPS 4 8 9 12

SMART TOYS
'Smart' or 'connected' toys are interactive and can be used by children from as young as three. They can be connected via Bluetooth or a Wi-Fi connection. As with any smart devices, you should check that the Internet connection it links to is securely set up, and that any apps it links to on your phone or tablet are securely configured.

SEE TIPS 5 6 8 10

SMART SECURITY DEVICES
Internet-connected security devices such as CCTV cameras, baby monitors, locks and doorbells are open to the same risks as other smart home devices, except cyber criminals can access live footage and possibly control your door locks. Learn how to set up smart security devices properly to protect your home.

SEE TIPS 3 5 8 10

SMART DEVICES
Smart home devices such as smart speakers and appliances (sometimes called Internet of Things or IOT) contain miniature computers that connect to your home network.

Cyber criminals can use these devices to spy on you or to commit other crimes.

Ensure security is part of your buying criteria when purchasing 'smart devices' and learn how to keep them updated and secure.

SEE TIPS 3 5 8 10

ONLINE ACCOUNTS & CLOUD SERVICES
Services you use online like shopping, social media, email, media streaming, and cloud services (e.g. photo/file backup sites) can be targets for cyber criminals, due to the personal data and financial information stored on them. Strong passwords and enabling 2 Factor Authentication can help protect your data.

SEE TIPS 5 6 7 10

A CYBER SECURE HOME

HAVE CONFIDENCE IN YOUR HOME SECURITY

A connected home is set up so that Internet-enabled appliances and devices like central heating, lighting, security cameras, baby monitors, TV's and kitchen appliances can be controlled remotely using a networked device such as a smart phone.

While a connected home is efficient and makes life a lot easier, there are security risks. If these 'smart' appliances and devices are not correctly set up and secured, cyber criminals could gain acess to them and potentially steal personal & private data and financial information that you store or access through your smart devices.

1.PHYSICAL SECURITY
• Store devices out of sight in safe places when not in use e.g. car or home

• Turn on a 'Find My Device' service so that lost or stolen devices can be located, and data can be wiped remotely if necessary.

• Regularly make a secure backup of your data separate from your computer, offline, and stored in a safe place.

2. KNOW YOUR NETWORK
• Change the default username and password on your Internet Service Provider's router and any other network devices you may have. Your provider should give you instructions on how to do this.

• Be aware of what is connected to your wired network and Wi-Fi using tools like the 'Fing' app. Some routers also have this feature built in. This will help identify any devices that should not be using your network.

3. SECURE YOUR WI-FI
• Never set your Wi-Fi network to 'Open'. Your Internet Service Provider should give you instructions on how to secure your Wi-Fi with 'WPA2' or 'WPA3' encryption standard.

• Change the default name of your Wi-Fi network (called the SSID) to something that won't disclose your Internet Service Provider's name (which can reveal the hardware you are using to cyber criminals).

• Change the default Wi-Fi password to something strong and hard to guess, and only share it with people you trust.

• Set up smart devices (e.g. your smart speaker) on a 'Guest' Wi-Fi network so that they are kept separate from devices that store private data, such as your PC or laptop. This reduces the risk of a hacker getting access to your main network through one of these devices. More information on how to do this can be found on our website information hub.

4. USE ANTI-VIRUS AND FIREWALLS
• Firewalls help stop unwanted Internet traffic and malicious apps using your network.

• Turn on the firewall included on your Internet Service Provider's router.

• Install an anti-virus package with built in firewall to secure each device against malware.

5. USE STRONG PASSWORDS
• Set strong passwords using three random words - longer is stonger.

• Ensure you have a strong password for your primary email because criminals could use this email account to get access to your other accounts using the 'Forgot Password' feature.

• Don't reuse passwords on multiple accounts.

• Use a password manager or your browser to store your passwords.

6. ENABLE 2 FACTOR AUTHENTICATION
• Use Two Factor Authentication (2FA) - this is essential and a way of 'doubling up' on security by verifying your identity using a code sent to your mobile phone, email address, or from an authenticator app.

7. SURF THE INTERNET SECURELY
• Use an up to date web browser such as Microsoft Edge, or Google Chrome.

• Check the address bar to make sure you are on the proper website you intended to visit.

• Only use reputable websites for shopping.

• Don't give more information that is needed to carry out a transaction.

• Consider more secure payment options – e.g. payment services like PayPal, or a credit card that provides additional buyer protection.

8. SECURE YOUR SOFTWARE
• Enable automatic updates for operating systems (e.g. Windows), apps, and anti-virus software - this will allow the latest versions to always be in place, minimising the risk of cyber attacks due to using out of date software.

• Only purchase and download software from reputable and trusted sources.

• Only buy devices from reputable retailers to ensure they adhere to safety and security guidelines

• If a device is no longer supported by the manufacturer, replace it with one that is.

9. BEWARE OF FAKE EMAILS AND TEXTS
• Scam emails (phishing) and text messages (smishing) that appear to be from reputable sources are known as social engineering. These are sent by cyber criminals trying to encourage the recipient to click on a dangerous website link, download malicious software or give out confidential data.

• Don't click on links, download attachments or take any other action if you're unsure about the sender of the email or text.

• Send suspicious texts to 7726 and phishing emails to report@phishing.gov.uk

10. SET UP PRIVACY CONTROLS
• Only allow necessary cookies for websites when you visit.

• Review privacy settings for apps on your devices and for services that you use online.

• Don't give more information than what is required to create an account or use a service.

• Make sure your social media accounts are set to private so that your information is not widely shared.

11. TURN ON PARENTAL CONTROLS
• Make sure there is a password or PIN for you to verify payments your children want to make, for example, in-game, or app purchases, otherwise they might purchase things above their age group.

• Set up content filters on devices that will block inappropriate websites.

• Talk to children about Internet safety. Useful resources on this can be found on our website information hub.

12. WORK FROM HOME SECURELY
• Be aware of your organisation's policies and procedures.

• Know how to report cyber incidents.

• Don't let family members use your work device.

• Accept software updates as soon as they appear on your device.

NI Cyber Security Centre

We work to make Northern Ireland cyber safe, secure and resilient for its citizens and businesses.

Contact us
info@nicybersecuritycentre.gov.uk

Visit our website
www.nicybersecuritycentre.gov.uk

Follow us on Twitter
@NICyberSC

In association with :-

scamwiseNI PARTNERSHIP

Version 1 - October 2021

Pocket Guide to

A CYBER SECURE HOME

Practical steps to help secure your connected home.

NI Cyber Security Centre

ALWAYS REPORT CYBERCRIME, ESPECIALLY IF YOU HAVE BECOME A VICTIM

PSNI
T: 101 (Non Emergency)
W: www.psni.police.uk

ACTION FRAUD
T: 0300 123 2040
W: www.actionfraud.police.uk

If you are in immediate danger and need assistance dial 999

VISIT OUR HOME SECURITY HUB FOR GUIDANCE AND TUTORIALS

SCAN ME

nicybersecuritycentre.gov.uk/home-security

USEFUL CONTACT NUMBERS

Contact Name	Rank	Role	Station	Mobile No.	Email
Ian Magee	Superintendent	District Commander	Coleraine	07801738790	Ian.Magee@psni.police.uk
Martin Reid	Chief Inspector	Performance	Coleraine	07917 176393	Martin.Reid@psni.police.uk
Rory Bradley	Chief Inspector	Engagement	Coleraine	07879693881	Rory.bradley@psni.police.uk
Colin Shaw	Inspector	Neighbourhood Policing Team	Limavady	07795152784	colin.shaw@psni.police.uk
David Burns	Inspector	Neighbourhood Policing Team	Ballycastle	07557 261 940	David.Burns2@psni.police.uk
Paul Patton	T/Inspector	Neighbourhood Policing Team	Coleraine	07540470208	Paul.Patton@psni.police.uk
Diane Roxborough	Inspector	Local Policing team - A	Coleraine/ Limavady	07920186765	Diane.roxborough@psni.police.uk
Tony Moore	T/Inspector	Local Policing Team - B	Coleraine/ Limavady	07764638360	Tony.Moore@psni.police.uk
Marty Mullan	T/Inspector	Local Policing Team - C	Coleraine/ Limavady	07917384635	Marty.mullan@psni.police.uk
Stephen McCafferty	Inspector	Local Policing Team - D	Coleraine/ Limavady	07920186765	Stephen.Mccafferty@psni.police.uk
Bjorn O'Brien	Inspector	Local Policing Team - E	Coleraine/ Limavady	07920186765	bjorn.obrien@psni.police.uk
Wendy Nixon	T/Sergeant	Community Planning	Coleraine	07796656962	Wendy.nixon@psni.police.uk
Mark Knowles	Sergeant	Neighbourhood Policing Team	Limavady	07827925603	Mark.knowles@psni.police.uk
Richard Jack	Sergeant	Neighbourhood Policing Team	Coleraine	07786888384	RichardJack@psni.police.uk.
Robert Ennis	Sergeant	Neighbourhood Policing Team	Ballycastle	07771357656	Robert.Ennis@psni.police.uk

Other useful numbers

IN AN EMERGENCY CALL 999

PSNI NON-EMERGENCY NUMBER IS 101

- **Crimestoppers –** 0800 555 111
- **24 Hours Domestic & Sexual Violence Helpline –** 0808 802 1414
- **Causeway and Mid Ulster Women's Aid –** 028 703 56573
- **Foyle Women's Aid –** 028 714 16800
- **Crime Prevention Officer –** 07764638397
- **COVID-19 COMMUNITY HELPLINE** 0800 802 0020
- **Childline –** 0800 1111
- **Action Fraud –** 0300 123 2040
- **Victim Support NI –** 028 713 70086

Causeway Coast and Glens PCSP Contact Details

Causeway Coast and Glens PCSP would like to hear your view on any aspect of Policing and Community Safety;

Coleraine: Cloonavin, 66 Portstewart Road, BT52 1EY

Ballymoney: Riada House, 14 Charles Street, BT53 6DZ

Ballycastle: Sheskburn House, 7 Mary Street, BT54 6QH

Email: pcsp@causewaycoastandglens.gov.uk 028 703 47034

Further information on the PCSP and its members can be found: www.causewaycoastandglens.gov.uk/live/policing-and-community-safety-partnership

THIS NEWSLETTER IS SUPPORTED BY THE NORTHERN IRELAND POLICING BOARD AND THE DEPARTMENT OF JUSTICE.

With thanks to PSNI for providing information in this leaflet.

All information stated is correct at time of print and is subject to change.