Newsletter

>THE E-NEWSLETTER FOR NEIGHBOURHOOD WATCH SUPPORTERS IN SUFFOLK

Welcome to the December edition of our newsletter.

It"s been another tough year but we hope that you can relax and enjoy your time with family and friends over the festive period.

Although preparations for Christmas may well be underway, don't drop your guard when it comes to keeping your home safe and secure, and please look out for your neighbours, especially the elderly.

The Suffolk Neighbourhood Watch Association would like to thank you for all the effort and support you have given to Neighbourhood Watch in the last year, and we wish you all a very safe and secure Christmas, and a happy new year.

We hope you enjoy the newsletter.

The Executive Committee

INSIDE THIS EDITION:

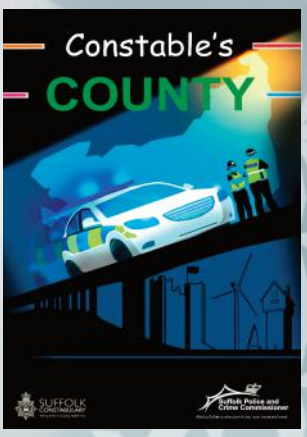
Have you got a story you would like to share?

Sharing your stories help give other schemes ideas that can help communities engage more. It's not always about crime and policing - but it's always about togetherness.

Send us your story via email to the Suffolk Neighbourhood Watch Association Comms team: comms@suffolknwa.co.uk

County Policing Command

Keeping people safe, catching and convicting criminals



The DECEMBER 2021 edition of the "Constable's County" newsletter is out now, and provides an update from across the East, South, and West of the county in a single edition. **Read it here**

The A to Z for Crime Prevention Advice

Iceni: Ipswich Charity receive funding award

Iceni, a small independent charity based in Ipswich, is one of only 27 organisations across the UK to be awarded the Respect Accreditation Standard for its Venta programme, which works with perpetrators of domestic abuse. The accreditation is the national benchmark for the provision of quality interventions with men who use violence against their female partners.

The programme has been jointly funded by Suffolk County Council and the Police and Crime Commissioner. Read more **here**

Suffolk Police and Crime Commissioner

Making Suffolk a safer place to live, work, travel and invest

Awards: £73.6k supporting local Crime Reduction Organisations

Five local organisations will share over £73k to fund various projects which contribute to reducing crime and disorder in the county or help victims or witnesses. Read more **here**.

A key part of the Police and Crime Commissioner's role is to commission services that support the Constabulary in its work and/or reduce demand.

For more detail on grants please **click here**.

Cyber Security: Get Safe Online

Get through this festive season safely. Visit www.getsafeonline.org for expert advice on how to stay safe online. **#safechristmas**

Scam: Advanced Fee Lottery Fraud

Over £925,000 was lost by victims in Advance Fee Lottery Frauds over the last seven months.

Victims reported losing an average loss of just over £1,500.

Lottery fraud occurs when criminals use fake messages and calls to convince a person that they have won a lottery or a prize draw. The victim is then informed that they will need to pay an advance "fee" in order to receive the winnings.

Victims are commonly asked to pay these advance fees by purchasing gift cards and relaying codes to the fraudster.

In some instances, victims have reported being asked for personal and financial information in order to obtain their "winnings". Some victims reported providing their bank details thinking they would be sent a small payment to verify the account. In reality, criminals use these details to steal the victims money.

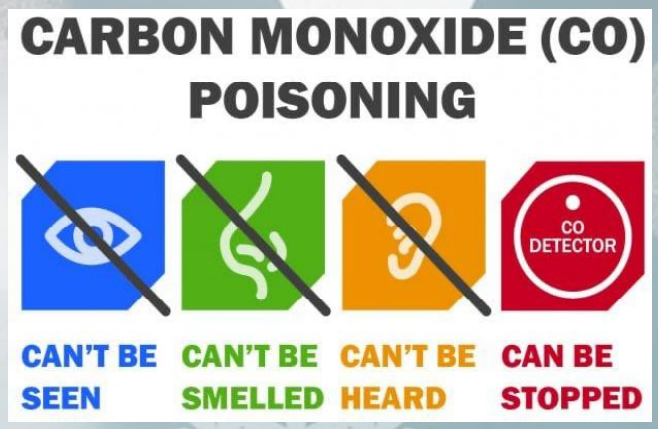
STOP: Unsolicited offers of large sums of money in return for a small upfront payment should always raise a red flag. Taking a moment to stop and think before parting with your money or information could keep you safe.

CHALLENGE: Could it be fake? After all, you can't win a prize in a competition you didn't enter. Remember, It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

Be wary of unsolicited callers instructing you to pay fees or fines using a gift card or voucher. Legitimate organisations would never do this.

PROTECT: Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

Home Safety: Carbon Monoxide Awareness



Carbon monoxide is a poisonous gas which has been linked to a range of long-term health conditions and complications, including low birth weight in babies, brain damage and heart disease. Many of us could be being harmed without even knowing, as carbon monoxide cannot be seen, smelled or tasted – this is why it is known as the 'silent killer'.

Carbon monoxide is produced when fuels such as gas, oil, coal and wood do not burn fully.

Burning charcoal, running cars and the smoke from cigarettes also produce carbon monoxide gas.

Gas, oil, coal and wood are sources of fuel used in many household appliances, including boilers, gas, fires, central heating systems, water heaters, cookers and open fires

Incorrectly installed, poorly maintained or poorly ventilated household appliances, such as cookers, heaters and central heating boilers, are the most common causes of accidental exposure to carbon monoxide.

It's important to be aware of the dangers and identify any appliances in your house that could potentially leak carbon monoxide.

Boilers, cookers, heating systems and appliances should be installed and regularly serviced by a reputable, registered engineer.

Do not attempt to install or service appliances yourself.

Anyone carrying out work on installations and appliances in your home must be registered with a relevant association, such as the:

Gas Safe Register (for gas appliances)
Heating Equipment Testing and Approval Scheme (HETAS) (for solid fuel appliances)
Oil Firing Technical Association (OFTEC) (for oil appliances)

Make sure all chimneys and flues are swept regularly by a qualified sweep who's a member of the:
National Association of Chimney Sweeps (NACS)
Guild of Master Chimney Sweeps
Association of Professional Independent Chimney Sweeps (APICS)

Carbon monoxide alarms are no substitute for an annual safety check by a Gas Safe registered engineer, however audible carbon monoxide alarms are a good second line of defence against carbon monoxide poisoning.

Carbon monoxide alarms are designed to sound when the concentrations of CO in the air are enough to harm you. A good CO alarm will sound when it detects the gas and it will be loud enough to alert everybody in the house. A CO alarm will sound when there are 50 or more parts per million (PPM) of CO in the air and alarms are designed to sound more quickly when higher and more dangerous concentrations of the gas.

Which? Report - Read more

Cyber Security: Buying Pets at Christmas

Scammers will try to take advantage of people looking to buy or adopt pets this Christmas. Don't get **#Petfished** and report any sellers you think might be deceitful to the RSPCA Cruelty Hotline on **0300 1234 999**

Fraud: Beware of NHS Covid Pass Fraud

Simple rule of thumb here is that the NHS Covid Pass id FREE!

The NHS will never ask for payment or any financial details.

For information on how to get your free NHS COVID Pass, please visit: https://nhs.uk/NHSCovidPass
Received an email or text which you're not quite sure about?

Is it asking you for payment or financial details?

If you are suspicious, you should report it by forwarding the email to: **Report@phishing.gov.uk**

Report suspicious text messages by forwarding them to 7726

Action Fraud: 12 Frauds of Christmas

This festive season, Action Fraud will be highlighting a different fraud type every other day to help you keep your money safe and out of the pockets of criminals this Christmas so you can enjoy a #FraudFreeXmas. #12Frauds

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Crimestoppers: Sexual Harrassment Survey

Crimestoppers and the University of Suffolk Centre for Abuse Research are asking about people's experiences of sexual harassment in public spaces through taking part in an online survey.

CrimeStoppers.
Speak up. Stay safe.

The research, **'Safe in public: understanding how sexual harassment affects people's use of public space'**, is seeking to learn more about people's experiences of sexual harassment in public spaces, how people think we should talk about these behaviours, and how people think we should respond to these behaviours to make public spaces safe and accessible. **Read more**

FIND OUT MORE ABOUT WHAT EXACTLY CONSTITUTES SEXUAL HARASSMENT, THE SIGNS TO SPOT AND HOW YOU CAN REPORT IT WHILST REMAINING 100% ANONYMOUS – GUARANTEED.

We all have a part to play in looking out for our neighbours, family and friends this winter. Do your bit and speak up to protect the people you love.

CrimeStoppers.
0800 555 111
100% anonymous. Always.

Ransomware Fraud: Emerging Threats

Ransomware, scams taking advantage of new habits, and fleeceware among the top threats of 2021

The pandemic has changed nearly every aspect of everyone's lives, and that includes the cybercrime world too.

Attackers' methods are becoming more sophisticated. They are using techniques that make their campaigns harder to spot. They are also carrying out more personalised attacks while adding new spins on tried-and-tested techniques, like social engineering. Here our Cyberhood Watch partner, Avast, takes a look at the most prevalent cyberthreats of 2021.

Ransomware, Sextortion and Scams
Cybercriminals used the pandemic to their advantage throughout 2021, spreading scams and phishing campaigns to exploit people's new online habits, responsibilities, and eagerness for Covid-related updates and information on vaccine rollout programmes.

They also launched ransomware attacks targeting consumers and critical infrastructure, including hospitals. Globally, Avast observed a 38% increase in ransomware attacks targeting consumers between June and October compared to the first five months of the year (January-May). In early 2021, Avast researchers saw a surge in sextortion scams, blocking over 500,000 attacks. These scams took advantage of the increased use of video conferencing services during the Covid-19 pandemic, falsely claiming to have accessed user devices and their integrated cameras.
People in several countries also received SMS messages linking to a banking Trojan called "FluBot", which impersonates parcel delivery companies in order to steal credentials and other personal data. Tech Support Scams (TSS), delivered as pop-ups or websites, were also widespread. TSS trick victims into believing their computer has been infected by malware and that they must call a technical support hotline to resolve the issue. However, these hotlines are run by cybercriminals who attempt to gain remote access to the device with the goal of stealing financial information. In general, phishing attacks continued to increase during 2021. Consumers remain the primary target, with the chances of encountering an attack growing by 20% between June to October.

Mobile threats continued to spread and diversify with lockdown restrictions
Adware is still the most significant threat on Android phones and tablets. Globally, 54.7% of mobile threats detected from January to September were adware. Fake apps came in second at 10%, banking Trojans in third at 9.6%, followed by downloaders (7.5%) and spyware (2.3%).
Fleeceware apps also proved to be a serious concern to users in 2021. Avast discovered more than 200 new fleeceware applications on the Apple App Store and the Google PlayStore. These apps promised free trials but ended up extracting money from their users through subscription services.

Looking back
Michal Salát, Threat Intelligence Director at Avast, says "Cybercriminals kept up many of their tricks this year, using social engineering to spread malware to get their hands on people's money, abusing technology such as stalkerware to violate people's privacy or deceiving vulnerable audiences into paying for fleeceware apps or unneeded tech support.".
Michal concludes "We are seeing increasing online harms that affect how people experience the digital world. Attackers' methods are becoming more sophisticated and everyone is being targeted, from everyday users to hospitals and oil pipelines to food companies globally. We hope by raising awareness around what we observed this year, we can help prevent people from falling victim in 2022."

To find out more about Neighbourhood Watch and Avast's joint programme, Cyberhood Watch, to tackle cybercrime, visit avast.com/uk- cyberhood#pc.

StreetSafe: Which streets do you feel unsafe in?

Are there streets near you where you don't feel safe? Do you avoid an alley or pathway at night because of poor lighting or encroaching bushes blocking the view? Does the sight of graffiti or abandoned vehicles in a particular area make you feel unsafe? Has the behaviour of others in an area caused you concern, e.g. being followed or verbally abused?

Even if a crime has not been committed, your safety and wellbeing is being affected. **Now you can report it, anonymously, via StreetSafe, so that something can be done about it.**

StreetSafe is a service provided across England and Wales by the Police on the **police.uk website**, to enable you to report streets in your neighbourhood where you don't feel safe, and identify the reasons for concern.

Using the reporting webform is simple and quick. All reports in a particular area can be accessed by your local police team, who will liaise with the local council, where necessary, on the actions to improve street safety. Street lighting can be added, overgrown hedges can be cut back, or the police can set up foot patrols at particular times of the day or night.

StreetSafe is not for reporting an actual crime– it is for reporting your concerns about your local environment or the behaviour of groups or individuals in a particular area and its impact on your wellbeing and the safety of you and other residents.

Suffolk Fire Service: Careful with Candles

Now the night's are drawing in

if you're lighting candles to add ambience this winter, remember to always put out any candles before you go to bed and never leave them unattended!

SUFFOLK TRADING STANDARDS

citizens advice

Friends Against SCAMS

www.friendsagainstscams.org.uk

REPORT IT, HELP OTHERS! #RogueFreeSuffolk

If you see a scam, an unsafe product, OR a Rogue Trader, report it via **0808 223 1133.**

Alert: Beware of Nottingham Knockers

There has been a number of reports to advise that Nottingham Knockers have been calling at properties across West Suffolk.

These individuals often claim to be on a youth offending or similar scheme, attempting to mend their ways, before trying to sell the householder everyday household products at very high prices.

Trading Standards always advise residents to refrain from buying at the doorstep and not to buckle to pressure from salespeople offering supposedly one-off 'buy it now' low prices.

Nottingham Knockers generally work in groups across the country but they are not involved in any officially recognised offender rehabilitation programme and many do not possess Pedlar's Certificates, which are issued by police.

If you are approached at the door, please refuse to buy.
Please report any doorstep caller to us via 0808 223 1133.

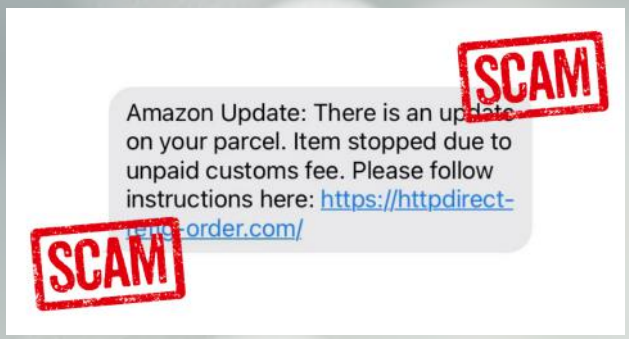
Scam: Courier Fraud

Fraudsters are preying on the festive season and relying on the fact that many people are buying online for Christmas.

They want access to your money and information, or for you to click on links which could download malware to your device.

Instead of clicking the link, log into your account directly to update or check your information.

If you receive a scam text message report it by forwarding it to 7726.



If you think you might have responded to a text message scam and provided your bank account details, contact your bank immediately. **Report all scams to Trading Standards via 0808 223 1133.**
You can forward scam text messages to 7726

Neighbourhood Watch Benefits

Beautifully secured by **Patlock**

Click here to order a Patlock at the Neighbourhood Watch discounted rate of £42.50

SPECIAL 15%DISCOUNT FOR ALL NWN MEMBERS

Use Coupon Code NWNLock on Check Out.

Visit www.locklatch.co.uk