

Newsletter

>THE E-NEWSLETTER FOR NEIGHBOURHOOD WATCH SUPPORTERS IN SUFFOLK

Welcome to the late April edition of our newsletter.

The Executive Committee have started preparations for the next Annual General Meeting, for which details will be sent out next month. This coincides with a call for new volunteers to come forward to take up roles on the committee. Watch out for further updates....

This edition looks at a number of scams for you to be aware of. You can help raise awareness by sharing the information.

As always, please remember to check our "news" page on our website for updated news in between newsletter editions, and if you use social media, why not visit our <u>Facebook page</u>, follow us and give us a "like".

We hope you enjoy the newsletter.

The Executive Committee

INSIDE THIS EDITION:

National Organisation news PG 2
Action Fraud PG 7
Cyberhood Watch PG 9

Trading Standards PG 4
Stop Loan Sharks Community Funding PG 8
Get Safe Online PG 10

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:



Thank you to all the schemes that send us their newsletters. You can send yours to comms@suffolknwa.co.uk

If you would like them uploaded to our website, just let us know!











Executive Committee: Planning begins for the 2022 AGM

Details of the next Annual General Meeting (AGM) shall be circulated via our newsletter and our website.

Scheme Coordinators represent their scheme members when voting at the AGM, and all the details will be found on our website via the Coordinator Login page., So please remember to check regularly for details being provided during May

At the same time the Suffolk Neighbourhood Watch Association are always seeking volunteers to come and join the Executive Committee to undertake roles which help support all the neighbourhood watch schemes across Suffolk.



There are a number of interesting roles for which we hope some volunteers will come forward to help in support of the Association.

In particular, we are looking for Event organisers, Parish Council Liaison, Area Network Coordinators, Social Media. More details will be provided on our website during May.

National Neighbourhood Watch: 40 Years, 40 Actions pack

In celebration of 40 years of supporting communities and reducing crime, Neighbourhood Watch are proud to share 40 actions to inspire you to connect more with your community. For ideas on raising crime prevention awareness, developing community cohesion, or building more inclusive networks, the "pack" can be found HERE. You can click on each activity within the document to find out more.

Get involved with as many actions as you like, or come up with your own!















National Neighbourhood Watch: The Neighbourhood Watch Journey

As a valued Neighbourhood Watch supporter, the National NW Organisation would like to share with you two exciting projects. Firstly, they are launching **OUR JOURNEY**, an interactive presentation that takes you into our past, present, and future. Secondly, an **INSIGHTS SURVEY 2022** gives you an opportunity to provide comment on how you think they are performing.



Explore the Neighbourhood Watch past, present and future journey

As you may already know, NW is celebrating the 40th anniversary of building stronger communities this year and the organisation is immensely proud of the journey that has been embarked on together during these four decades to get to where we are today. It goes without saying that this couldn't have been acheived without the support of the public and the unwavering support of the dedicated army of volunteers, some of which have been volunteering with NW for the entire 40 years.

The journey through the past 40 years demonstrates the importance of neighbours coming together to build strong and resilient communities. Over the years, our communities have faced significant challenges from economic crises, cyber threats, floods and pandemics. We know that together, we are stronger, so to celebrate this landmark anniversary, NW has launched an interactive timeline reflecting our rich past, strong present position, and future ambition to be the authoritative voice on community-based crime and the first step in connecting communities.

VIEW OUR INTERACTIVE TIMELINE

But you don't have to take their word for it; you are invited you to let them know what you think

The past 40 years have seen the introduction of the internet, the opening of the Channel Tunnel, the first women priests in the Church of England, civil partnerships for same-sex couples, and seven different prime ministers. We believe we've remained relevant throughout this time by adapting and responding to the changing needs of communities and crime.

But what do you think? To find that out, NW are running a short survey across England and Wales for members and non-members alike. Your answers will be anonymous and help NW identify positives that can be built on and areas where NW may need to do better. To add to this, you could be in for a chance of winning £25 by completing the survey.

The survey will be open for three weeks (25th April – 15th May 2022), and initial results will be shared at the Neighbourhood Watch National Crime Conference held on 31st May 2022.

TAKE PART IN OUR INSIGHTS 2022 SURVEY

25th April - 15th May 2022

Please spread the word - NW wants to gain the broadest possible range of responses representing the diversity of England and Wales, especially those in cities and high crime areas. Please help by sharing this survey link with your friends, family and networks. Forward this via email, or post this link https://www.surveymonkey.co.uk/r/InsightsNW to your WhatsApp or social media groups.

NW thank you for your ongoing support!

















Suffolk Trading Standards: Scams, Scams, Scams

A resident in Eye has received a call from someone purporting to be from Trading Standards. The caller said they were working from home and needed to come and discuss a complaint about the consumer's solar panels. The resident has not made any such complaint and the caller was quite persistent.



As with any telephone call that you receive out of the blue, we urge you to be vigilant and take a moment to stop and think, especially if you receive a request over the phone or e-mail to make a payment from someone claiming to be from a trusted organisation. If you are in any doubt, contact the company or organisation directly using an email or phone number from their official website.

Impersonation scams occur when the victim is persuaded to make a payment to a criminal claiming to be from a trusted organisation. This could include the police, a bank, a utility company, or a government department.

There were almost 15,000 impersonation scam cases reported nationwide by UK Finance members between January and June this year, an increase of 84 per cent compared to the same period last year. Losses during this time amounted to £58 million, an increase of three per cent on last year.

Report all scam calls to us via Citizens Advice Consumer Service on 0808 223 1133.

In another scam, a Lowestoft resident had a call from an individual claiming to be from their water company.

The fraudster claimed the resident had overpaid their water account and so they needed their bank details to be able to refund them.

The caller was very persistent, offering to wait until the resident got their bank statement or bank card.

Thankfully the resident was suspicious of the call and refused to give them their financial details, demanding that they send a cheque with the overpayment. They then hung up.



If you receive a similar call, please hang up and do not provide the caller with any personal details.

Essex and Suffolk Water can be contacted on 0345 782 0999. The company offer a password protection scheme through its Priority Services Register. This scheme means that any customer can choose a secure password and if they were to get a visit or call from the water company they can confirm who they are with this, only genuine employees from Essex & Suffolk Water would know the password.

Anglian Water can be contacted on 03457 145 145. Their customer contact staff will be able to check and make sure any telephone call, doorstep call or email are genuine and will be able to advise you on billing.

If you have given a scammer any financial information, please contact your bank immediately.











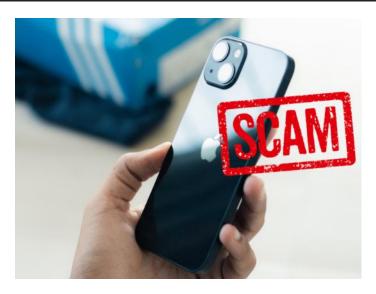
Suffolk Trading Standards: Scams, Scams, Scams

A Sudbury resident has become a victim of an iPhone delivery scam.

They returned home from work to find that an iPhone 13 had been delivered to their address, in their name, which they had not ordered.

The resident contacted the phone provider and was able to establish that they had been a victim of identify theft.

Looking back at their CCTV they could see that the package was delivered by a courier and posted through the door. Moments later the property was approached by a man who knocked on the door. As the resident was out, the fraudster was unable to collect the package.



This is a common scam where fraudsters take out mobile phone contracts using the victim's details, without their knowledge or consent. The scammer then tries to intercept the delivery, or trick you into handing over the high value package.

How to stay safe

If you receive a package you cannot remember ordering, do not hand it over if a courier requests it.

You should check their credentials and call the company they represent to check if they are legitimate, and potentially call the police.

The next step would be to contact the retailer as soon as you can to arrange for the package to be sent back.

If you are targeted by this scam, it's a good idea to tell your bank as your details could be compromised and you may be a victim of identity theft.

Protect yourself against identity fraud

Don't throw out anything with your name, address or financial details without shredding it first.

If you receive an unsolicited email or phone call from what appears to be your bank or building society asking for your security details, never reveal your full password, login details or account numbers. Be aware that a bank will never ask for your PIN or for a whole security number or password.

Check your statements carefully and report anything suspicious to the bank or financial service provider concerned.

Don't leave things like bills lying around for others to look at.

If you're expecting a bank or credit card statement and it doesn't arrive, tell your bank or credit card company.

If you move house, ask Royal Mail to redirect your post for at least a year.

These credit reference agencies offer a credit report checking service to alert you to any key changes on your credit file that could indicate potential fraudulent activity: TransUnion, Equifax, Experian, ClearScore, Noddle

It is particularly helpful to check your personal credit file 2-3 months after you have moved house.











Suffolk Trading Standards: Scams, Scams, Scams

Suffolk Trading Standards have received a few reports of what appear to be bogus doorstep callers, calling at properties in lpswich to talk about Broadband pricing.

At one property they were very persistent, claiming that they were not selling, but wanted to talk to the resident about broadband pricing. At another they stated they were there to talk about "fibre upgrades". Here it was noted that the male had a jacket with the name of a company on it, but for a different type for business. One other reported that the caller claimed to work for a broadband provider but was unable to provide any ID.



Were you approached? If so, please call Suffolk Trading Standards to provide any further intelligence.

If you do have someone knock at your door:

Use a spy hole, chain or window to have a look at the caller before answering the door and keep the chain on. If you do not recognise the caller then speak through the closed and locked door.

Always ask for proof of identity. Take it from the person (through the letterbox) and read it carefully before deciding what to do.

Never use a phone number provided by the caller as it could be a false number to an accomplice.

Never give bank details to a caller, even those claiming to be from charities. Police will have a list of charitable organisations visiting your area which can be checked by calling 101. We recommend that you contact the charity directly if you wish to make a regular donation through your bank or building society.

Display a No Cold Calling sticker on your door which are free from Trading Standards and never buy goods and services from people calling at your door.

If you have any doubt, keep them out and remember you do not have to open the door.

Report all doorstep callers to Suffolk Trading Standards via Citizens Advice Consumer Service on 0808 223 1133.









Action Fraud: Remote Access Scams

Action Fraud National Fraud & Cyber Crime Reporting Centre 10300 123 2040

Over 20,000 people fell victim to remote access scams

More than £50 million was lost last year to scams where victims are tricked into handing over control of their computer or smartphone to criminals.

New data from Action Fraud reveals that 20,144 people fell victim to scams where they were persuaded to grant criminals remote access to their device.

Victims reported losing a total of £57,790,384 – an average loss of £2,868 per victim.

What are remote access tool scams?



Remote access tool scams will often begin with a browser pop-up saying that your computer is infected with a virus, or with a call from someone claiming to be from your bank saying that they need to connect to your computer in order to cancel a fraudulent transaction on your account.

Criminals will try to persuade the victim to download and connect via a remote access tool, which allows the criminal to gain access to the victims computer or mobile phone. If the victim allows the criminal connection via the tool, they are able to steal money and access the victims banking information.

How to protect yourself

Only install software or grant remote access to your computer if you're asked by someone you know and trust, such as a friend or family member, and never as a result of an unsolicited call, browser pop up, or text message.

Remember, a bank or service provider will never contact you out of the blue requesting remote access to your device.

If you believe your laptop, PC, tablet or phone has been infected with a virus or some other type of malware, follow the NCSC's guidance on recovering an infected device https://www.ncsc.gov.uk/guidance/hacked-device-action-to-take

Protect your money by contacting your bank immediately on a different device from the one the scammer contacted you on.

Action Fraud also advises that the public follow the advice of the Take Five to Stop Fraud campaign to keep themselves safe from fraud:

Stop: Taking a moment to stop and think before parting with your money or information could keep you safe.

Challenge: Could it be fake? It's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

Protect: If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online at https://www.actionfraud.police.uk or by calling **0300 123 2040**.









England Illegal Money Lending Team: Community Funding

STOPLOANSHYRKS

Intervention . Support . Education

The England Illegal Money Lending Team (IMLT) have launched the latest round of their Stop Loan Sharks Community Fund with a share of £160,000 funding up for grabs.

Charities, community groups, schools, and organisations from the public, private and voluntary sectors are able to apply for proceeds of crime funding for projects that raise awareness of the dangers of loan sharks and help make communities safer.

Grants of up to £5,000 are being made available with collaborative bids between multiple agencies being considered. Projects must raise awareness of the dangers of loan sharks, help to reduce crime and disorder and have a positive impact on local communities.



The funding comes from money recovered from convicted loan sharks under the Proceeds of Crime Act (POCA).

There has never been a more important time to raise awareness of the devastating impact illegal money lending has on victims and their families and highlight the support available to those affected.

As the cost of living continues to rise and more people face increased hardship, there are concerns that loan sharks will look to exploit the most vulnerable struggling to make ends meet.

In a new report published last month, Swimming with Sharks, the Centre for Social Justice (CSJ) reveals that there could already be up to one million people in debt to loan sharks in England, with some lenders demanding sexual favours as repayment from borrowers.

Over £2.5 million has been given to more than 600 deserving projects so far since the Stop Loan Sharks Community Fund launched over 10 years ago.

Details on how to apply for the funding can be found at https://www.stoploansharks.co.uk/poca-funding

The closing date for applications is **Thursday**, **June 30**.







Cyberhood Watch: The era of the swindler?

Netflix shows such as The Tinder Swindler and Inventing Anna are highlighting how sophisticated scammers can be.

As part of the <u>Cyberhood Watch</u> programme, Avast is encouraging local communities to be on the look-outfor fraudsters pretending to be friends or family, or from services such as Amazon and Netflix.

Earlier this month, research carried out by Avast found that 62% of British adults have been targeted by fraud at least once in their lifetime, and 57% are worried about being scammed online. While nearly half of those we surveyed said they had been targeted by fraudsters pretending to be services such as Netflix and Amazon, 40% experienced impersonations by people posing as friends, while over a third were led to believe it was their partner.

For example, the findings showed that one in five people have been targeted by 'romance fraud', the act of someone you are interested in pretending to be someone else or trying to gain your affection for their own benefit.

Around a quarter (25%) of the respondents in the survey said they had been asked for money by someone they had only met online, and of those almost a half (44%) had coughed up the cash. Similarly, over a fifth (22%) said they had been asked to transfer money to someone they thought they knew, only to discover the request was a fraudulent one.

Jaya Baloo, Chief Information Security Officer at Avast, comments: "Sadly, we were not surprised to see that over half of Brits are worried about being scammed online. The reality is that online scammers have no scruples and are always seeking to exploit peoples' emotions, circumstances or events in their lives, in order to make money.

The fraudsters are increasingly getting more sophisticated, so we urge people to think twice before sharing personal information online or clicking on links which could be clever impersonations from fraudsters. We want to give people the tools and knowledge they need to stay safe and enjoy their digital freedom online."

Here are the telltale signs of a typical scam:

- You're being approached by someone you've never actually spoken to or met in person
- They open with a request: "I need your help"
- They emphasise the urgency of the situation or apply time pressure
- Poor grammar, spelling and spacing
- They ask you to click on a link, or send money directly
- For more information on how to stay safe online and to spot the signs of online fraud visit: https://blog.avast.com/avoid-scams-while-helping-loved-ones-avast

If you think you'd be a good fit for the Cyberhood Watch Ambassador volunteer role, email enquiries@ourwatch.org.uk for more information.











Get Safe Online Organisation: Tips to avoid holiday scams



The internet is by far the most popular place to research and book holidays and travel, but it's also a favourite for fraudsters, constantly trying to scam us with holidays, accommodation and travel that don't actually exist.

With fake listings, emails, social media posts, texts and other ads which can look very authentic, it can be difficult to tell if you're going to get that hard-earned break or end up sitting at home.

To avoid becoming a victim of holiday and travel scams, start by reading our top tips. Visit www.getsafeonline.org

#holidaybooking





www.getsafeonline.org













And Finally: Refugee Week 2022

Refugee Week 2022 is coming, and you can take part by holding your own event or activity, big or small, 20th -26thJune.

The Refugee Week 2022 Event Organiser Pack, has all the info, tips and resources you need to get started.

Refugee Week is an annual festival celebrating the contributions of refugees, and the theme for 2022 is 'Healing'.



Every year, hundreds of people and organisations across the UK and the world hold all kinds of activities that bring people together and encourage understanding of refugee experiences – from craft workshops to community walks, and everything in between!

Whether you take part in your neighbourhood, with a group or organisation or simply with friends, you'll be part of a growing global movement proudly celebrating sanctuary and the possibility of new beginnings.









