Newsletter

>THE E-NEWSLETTER FOR NEIGHBOURHOOD WATCH SUPPORTERS IN SUFFOLK

Welcome to the March edition of our newsletter.

We would like to start off by apologising for the lack of newsletter for February. Unforeseen circumstances meant we were unable to produce the newsletter within the timescale. As such, we need to announce that our current Chair, Tony Spall, has stood down from the role of chair due to family commitments, but continues to offer a level of support with our various communication channels. The Executive Committee will share the responsibility of the Chair position until such time a new person is elected to the role.

With a planned route out of the lockdown and the vaccination programme moving forward successfully the outlook is far more positive than it has been for some time. As this coincides with springtime there seems to be the beginnings of a more optimistic outlook and a return to something approaching normal life. While this is a definite improvement, we know there are still lots of vulnerable people in our communities struggling with the current situation. The great work of Neighbourhood Watch in supporting them and helping to protect all our communities from crime is as vital as ever.

The March edition particularly focuses on all the Scams that we are facing on a regular basis, and more so during the pandemic.

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 Facebook page, follow us and give us a "like".

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

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!

Reaching Out: Suffolk Association of Local Councils

The pandemic has proven to be very difficult times for us all, especially for those that have suffered personally thorough contracting Covid 19, or even worse the loss of a family member or friend to the dreadful disease.

The last twelve months have highlighted the skills and kindness of not only the NHS and Key workers, but also the volunteers in local communities offering their help and support with acts of kindness.

We in the Suffolk Neighbourhood Watch Association (SNWA) have seen many examples of this by our members who have either organised or been part of local teams created especially to help those people in their local community. There have been some wonderful examples of schemes reaching out to their neighbours during the pandemic and periods of bad weather, where circumstances have prevented some from being unable to shop or collect prescriptions, or other simple, basic, but nonetheless essential tasks.

These acts of neighbourliness are core to the values of the Neighbourhood Watch (NW) movement, and is why we we are always keen to engage and expand our membership.

A number of our NW schemes have members who hold positions on their local Town or Parish councils, and this ensures a good representation of NW. But not all councils have NW members, and so we have recently written to the Suffolk Association of Local Councils (SALC) as the organisation which supports and represents the corporate interests of town and parish councils and meetings across Suffolk, asking for their help.

SALC have kindly agreed to include a letter and questionnaire from SNWA in their latest newsletter, asking each Town/Parish council to confirm or explore their relationship with NW. The article can be found on our website **here**

As this communication has only just been started it will be some time before we can expect any results.

If you have contacts in to your local town or parish council, we would be grateful if you could ask them to help us by completing the survey.

Any queries can be emailed to enquiries@suffolknwa.co.uk

Neighbourhood Watch Network: National news

At a recent Board Meeting, the NWN Trustees approved the 2021/22 Budget which includes confirmation that the Home Office will continue to fund NWN at the same level as last year.

This is a real endorsement of the work across the organisation over the past year to provide evidence of the impact of Neighbourhood Watch, which has been highlighted in the 2019/20 Impact Report. Continuing to collect evidence and data on the impact of Neighbourhood Watch will be a key part of NWN work this year. The NWN team will be working with Area Associations to devise a way to collect data from local areas to better illustrate the value and impact of having schemes and being a part of Neighbourhood Watch.

The NWN team also welcome a new staff member, Esther Ardagh-Ptolomey, who recently started in her role as the Volunteer Development Manager. The role is initially a 6-month contract and is funded by the National Lottery Emergency Covid-19 Response Grant. Esther comes with a wealth of experience in volunteer-led organisations and will be working to develop the Volunteer Programme for the organisation, which will include training, support, role development, and resources.

Suffolk Police & Crime Commissioner and Suffolk Constabulary: CoPaCC Award

Suffolk Police and Crime Commissioner

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

Suffolk Police and Crime Commissioner's office has been awarded a prestigious national award for openness and transparency for the sixth successive year.
The quality mark has been awarded by CoPaCC, an independent national body which monitors police governance and recognises excellent performance by Police and Crime Commissioner's and their offices.

Neighbourhood Watch Week 2021: Save the date!

Staying safe from email scams

Fraudsters are constantly coming up with new ways of trying to defraud people in relation to all manner of products and services, including loans, dating, holidays, business opportunities, clairvoyants, pharmaceuticals, lottery prizes, fake COVID vaccines, even recovery of money lost to fraud and a whole lot more.

Here we look into some of the different types of email frauds that are currently quite common and what to look out for to indicate that an email may not be genuine.

COMMON TYPES OF EMAIL SCAMS

- **419 Emails:** You are offered a share in a large sum of money in return for helping to transfer it out of the country. Once you have given the criminals your bank account details, they empty your accounts.
- **Phishing:** An email that purports to be from companies such as banks designed to trick you into revealing your personal informationand passwords.REMEMBER: your bank will NEVER contact you out of the blue to ask for your PIN, full password or to move money to another account.
- **Pharming:** Pharming is a term used when you are directed from a link in an email to a website that spoofs a legitimate website in order to access your personal details.
- **Impersonation of UK official websites:** For example HMRC, with an email message claiming you are due a refund and requesting your bank account details or directing you to a website link.
- **Impersonation of UK officials:** Criminals impersonate a UK official to obtain personal information and steal money, often claiming that you are due a refund or must make an urgent payment. Examples of this scam include TV License, the HMRC Tax Rebate and the Council Tax Scam.
- **Investment scams and pension scams:** Emailed offers of worthless, overpriced or non-existent shares, or a time-limited opportunity to convert some or all of your pension pot into cash. Click here to find out more about these.

HOW TO SPOT A SCAM EMAIL

- The sender's email address looks suspicious. Roll your mouse pointer over the sender's name to check it. If it **doesn't match** the website address of the organisation it says it's from it could be a sign of a scam.
- The email **doesn't use your name** – it says something like 'Dear customer' instead.
- There's a **sense of urgency**, asking you to act immediately.
- There's a prominent website link that may look at first glance like the proper address but has **one letter missing or is spelt wrong**.
- There's a **request for personal information**.
- **Poor grammar and spelling mistakes**.
- The **entire text of the email is contained within an image** rather than the usual text format, and the image contains an embedded hyperlink to a bogus site. Again, roll your mouse pointer over the link to reveal its true destination. **But don't click it!**

Staying safe from email scams

It is almost impossible to keep up with the variety of fraudulent emails that are increasingly appearing on our computer screens and smartphones. However, by taking your time and following the simple steps below you can better protect yourself from falling victim to attempted email fraud.

REMEMBER: IF SOMETHING SEEMS TOO GOOD TO BE TRUE, IT USUALLY IS!

1. Create a **separate password** for your email accounts
2. Make sure you have **strong passwords with three random words** and change these regularly. Find out more about **strong passwords** here
3. Install **two-factor authentication (2FA)** for your email accounts. This is an additional process to secure your account.

Further actions you can take to keep safe

Look after your **mobile devices**. Don't leave them unattended in public places, and protect them with a PIN or passcode.

Ensure you always have **internet security software** loaded on computers and update to new versions immediately.

Don't assume that **Wi-Fi hotspots** in places like cafes and hotels are secure. Never use them when you're doing anything confidential online, like banking. Use 3G or 4G.

Never reveal too much personal or financial information (such as in emails, on social networking and dating sites). You never know who might see it or use it.

Always consider that online or on the phone, people **aren't always who they claim to be**.

Fake emails and phone calls are a favourite way for fraudsters to approach their victims.

Don't click on links or open attachments **if the source isn't 100% known and trustworthy**, or it seems strange that you'd be receiving them.

Always access internet banking sites **by typing the bank's address** into your web browser.

Never pay for anything by direct bank transfer unless it's to someone **you know personally and is reputable**.

Never respond to emails, texts, letters or social media **that look suspicious,** including messages with **bad spelling or grammar.**

Be cautious when going to a website from a link in an email and then enter personal details – **the email could be fraudulent.**

If someone you've never met in person asks you for money, that should be a **red flag**. Tell them you're not interested and stop all contact.

When shopping online always sign up to American Express SafeKey, Verified by Visa and MasterCard SecureCode so look for the padlock or unbroken key symbol when you first visit a site. Where possible **make your purchase with a credit card** or via a credible online payment system (such as PayPal) which protects you in the event of fraud.

Sextortian scams: Stay calm and Ignore them

Sextortian scams surge during pandemic

In January this year, Avast threat researchers blocked over 500,000 attack attempts from cybercriminals claiming to have recorded videos of unsuspecting victims during private moments online. These attacks, known as sextortion scams, attempt to blackmail victims by threatening to make these apparent recordings public unless a payment is made to the scammer. Avast threat labs researchers advise people to **stay calm and ignore sextortion emails** instead of reacting to them, as they **usually are fake claims**.

Cybercriminals have been using the increase in video conferencing services during the Covid-19 pandemic to validate their false claims and provoke a reaction from the victim. The fraudsters allege to have taken advantage of critical vulnerabilities in the Zoom application, allowing them to access a user's device and camera. It is important to note that Avast has **not found any actual vulnerabilities in the Zoom application.**

"Sextortion scams are dangerous and unsettling, and can even have tragic consequences resulting in the suicide of affected users. During the Covid-19 pandemic, cybercriminals likely see a strong opportunity for success as people spend more time using video conference applications and in front of their computer overall," said Marek Beno, malware analyst at Avast.

"As scary as such emails may sound, we urge people to stay calm if they receive such a message in their inbox and ignore it, as it is just a dirty trick that cybercriminals use to try to get your money."

Another common sextortion campaign identified by Avast is an email in which the attackers claim a Trojan was installed on the recipient's machine, which has recorded their actions with a microphone and webcam, and extracted all data from their devices including chats, social media and contacts. A ransom is demanded and often includes a note about a fake "timer" that started when the email was received in order to set a ransom deadline. This campaign is also fake and uses social engineering to coerce people into paying.

Read the full article to find out how to recognise and protect yourself from sextortion emails.

Get Safe Online: Beware of vaccination scam

Don't get caught out by a COVID-19 vaccination scam

You may have read that fraudsters are taking advantage of the NHS COVID-19 vaccination programme. Typically, people are receiving emails, text messages or phone calls with offers to 'jump the queue' in return for payment or confidential details.

There is no charge for the COVID-19 vaccination, and the NHS is adhering rigidly to the government's order or priority list, so any such messages you receive are fraudulent.

For full information on protecting yourself against COVID-19 vaccination scams, visit **www.getsafeonline.org/vaccinationscams**
And please, pass on our advice to anyone you think may be caught out.

#vaccinationscams

GET SAFE ONLINE .org TM

Suffolk Fire & Rescue Service: Top Tip

SUFFOLK FIRE AND RESCUE SERVICE

NEIGHBOURHOOD WATCH TOP TIPS

FIRE KILLS
YOU CAN PREVENT IT

In the event of a fire in your home, ensure that everyone in your home knows what to do:

Get out…. Stay out…. Call 999

SUFFOLK TRADING STANDARDS

citizens advice

Friends Against SCAMS

www.friendsagainstscams.org.uk

XXX

Social media adverts offering to "flip" your money may seem like an easy way of making some quick cash but don't be fooled!

Criminals use money mules to launder the proceeds of their crimes by asking you to receive money into your bank account and transfer it into another account, keeping some of the cash for yourself.

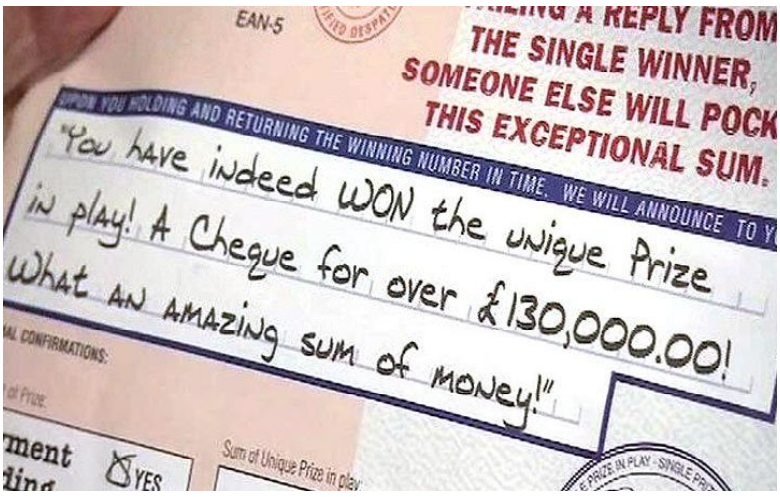
Allowing your account to be used for money muling will result in its closure, difficulty getting a credit or mobile phone contract, and in some cases, a prison sentence of up to 14 years.

You can stay safe by ensuring you don't allow anyone you don't know and trust to access your bank account. If you've been contacted by a role directly, make sure you know what it entails by conducting your own research.

Learn more here: https://moneymules.co.uk/

Is an older person in your family receiving more junk mail than usual?

Encourage them to stay #scamaware and stop, report and talk if you think they could be being scammed.



It's important to be aware of new scams due to the pandemic

If you need advice about a scam, you can contact the #ScamsAction service by phone or online chat.

More information can be found here

Need help with online scams?

Call the Citizens Advice Scams Action team

0808 250 5050

NHS Text Messages: Look out for scams

The NHS will soon start sending text messages to some people to invite them to book a COVID-19 vaccine appointment.

Almost 400,000 people aged 55 and over and 40,000 unpaid carers will be the first to get a text alert inviting them to book a slot as part of the latest development in the NHS vaccination programme, the biggest in NHS history.

The messages will include a web link for those eligible to click and reserve an appointment at one of more than 300 large-scale vaccination centres or pharmacies across England.

Reminders will be sent 2-3 weeks after the original alert to encourage people to get their vaccine if they have not taken up the offer.

Texts will arrive in advance of the standard letter, meaning if the trial is successful the solution could enable the NHS to react faster to changing vaccine supplies and fill appointments quickly.

In some cases text messages have been used by scammers to try to collect personal details from people, get them to ring premium rate numbers or enter their banking details.

The text message will be sent using the Government's secure Notify service and will show as being sent from 'NHSvaccine'.
Remember, the NHS will never ask you for payment or banking details in order to receive the vaccine.

If you receive an email, text message or phone call purporting to be from the NHS and you are asked to provide financial details, or pay for the vaccine, this is a scam.

For more info, visit: https://www.actionfraud.police.uk/alert/13587

Suffolk Crimestoppers: Report Crime Anonymously

CrimeStoppers.

Speak up. Stay safe.

With the first signs of the latest national lockdown beginning to ease, although the pandemic remains very much still active, we're appealing for people to report anonymously what they know about crime against commercial outlets.
As local shops and businesses try to cope with the devastating financial impact of the pandemic, the last costly disruption they need is having premises ransacked, with essential items or equipment damaged or stolen. It's not just burglary that affects businesses. Fly-tipping and arson can seriously impact a company's ability to reopen. For some, it could be the final straw.

The #ClosedtoCrime campaign is asking people to report what they know about crime against local businesses, from shops to company premises, factories to warehouses. They play a crucial role in the fabric of society – indeed, many staff in these businesses are now classed as key workers, providing essential services.

ActionFraud

National Fraud & Cyber Crime Reporting Centre

0300 123 2040

What is fraud?

Fraud is when somebody lies, or deceives you, in order to cause harm, usually by stealing your money.

What is cyber crime?

This is when fraudsters target computers, tablets or phones or use the internet to swindle you. Our increased use of electronic devices for everyday activities means that cyber criminals have a wealth of opportunity to commit crime.

What is Action Fraud?

Action Fraud is the UK's national reporting centre for fraud and cyber crime. Members of the public, businesses and charities can report to Action Fraud online or on the phone.

Victims' reports are assessed by specialists to see if they are suitable for further action and are then sent to the relevant law enforcement agency to investigate.

What should I do if I'm a victim of fraud or cyber crime?

You can report fraud and cyber crime using the online reporting tool:

www.actionfraud.police.uk

(24 hours a day, 7 days a week)

If you do not have internet access, or if you require more support, you can also contact Action Fraud on 0300 123 2040 to speak to an advisor.

Why do people in the UK report fraud and cyber crime to Action Fraud instead of the police?

Action Fraud takes reports from victims nationwide providing a clear picture of the scale of fraud and cyber crime, allowing law enforcement to link crimes which happen across the country. This kind of intelligence is the key to disrupting cyber crime.

If you are at all suspicious, heed your instincts!

You are most probably right to be concerned.

Report all emails that you believe to be fraudulent to report@phishing.gov.uk.