Newsletter

>THE E-NEWSLETTER FOR NEIGHBOURHOOD WATCH SUPPORTERS IN SUFFOLK

Welcome to the July edition of our newsletter.

We start this newsletter by reminding our members that they have until the 16th July to cast their online vote at the Annual General Meeting (AGM) for the Suffolk Neighbourhood Watch Association.
This vote provides access to the Chair's and Treasurer's reports with a link to a website where members can comment on the reports, as well as vote for any nominated Executive Committee Officers.
Your vote is very important to the success of the AGM.
The link to cast your vote is **here**.

Following this, the results of the AGM will be published to members. This will take place no later than 23rd July.

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:

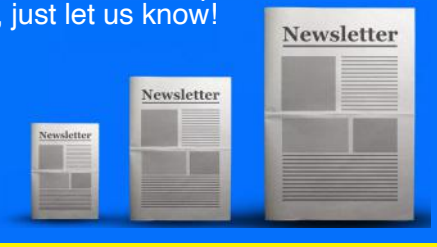
Have you got a story you would like to share?

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.

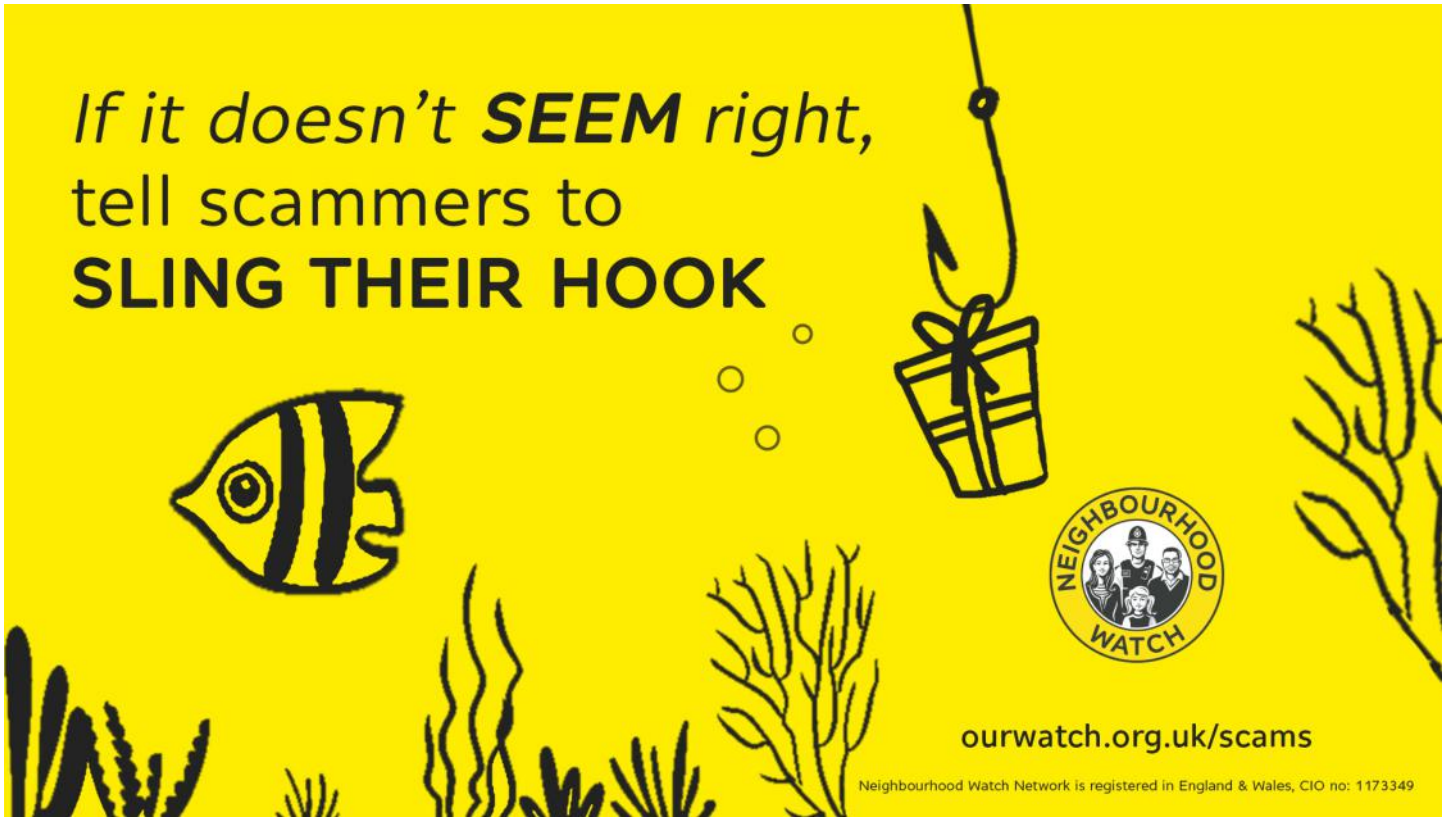
Send us your story via email to the Suffolk Neighbourhood Watch Association Comms team: comms@suffolknwa.co.uk

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!



Tell scammers to SLING THEIR HOOK!



SLING YOUR HOOK

The pandemic and successive lockdowns have sadly led to an increase in scams.
In response the Neighbourhood Watch Network (NWN) have launched a new campaign named **SLING YOUR HOOK** to help tackle scams. The campaign taps into the psychology that scammers use to hook people in, helping you stay one step ahead and protect yourself and loved ones against the increasing variety of scams that are happening everyday.
NWN have identified the following five behaviours scammers commonly use:
• They imply they're doing you a favour (reciprocity)
• They indicate everyone else is doing this (social proof)
• They say your only chance is to act now (urgency)
• They act like they're similar to you so you like them and want to please them (connection)
• They ask you to do one little thing which makes you do more (commitment).

NWN also know that often victims of scams report that in hindsight they felt something wasn't quite right at the time. This campaign aims to raise awareness of the tactics scammers use and encourages people to 'stop and think' if something doesn't FEEL, SEEM, LOOK or SOUND right. This allows them time to trust your gut instinct and help prevent becoming a scam victim.

A message from John Hayward-Cripps, CEO of Neighbourhood Watch Network:
"Everyone likes to feel special. But watch out! If a stranger is going out of their way for you, something fishy may be going on instead. Scammers like to offer one-off deals and favours. Don't be afraid to tell them no."

As part of the campaign NWN are running a number of free online talks, which are open to anyone to attend - details below.

The topics are:
• 23rd July, 5pm: Scams awareness training from the Friends Against Scams initiative
• 30th July, 5pm: Don't get hooked by scammers! What you need to know about flubot and phishing scams

To book please visit https://www.ourwatch.org.uk/webinars

Partnership with Deliveroo launched to train riders in community safety

On 10th June during Neighbourhood Watch Week, NWN launched a new project partnership with Deliveroo, providing their riders training to help keep communities safe across the UK. The optional training, created by Neighbourhood Watch and verified by the Metropolitan Police, will cover six topics over as many months, in the form of animated videos and simple quizzes.

The partnership forms part of Deliveroo's new 'Full Life' campaign which launched last month, in which the company pledged to 'use [their] network as a force for good', and is in response for calls amongst their riders and staff to increase education in community safety. The topics are: rider vehicle safety, street harassment and female safety, domestic abuse, handling confrontation and bystander training, modern slavery and human trafficking, and county lines and drug dealing.

Alexandra Holmes, a Deliveroo rider said: "I am really pleased that Deliveroo is offering this free training for riders and hosting roundtables to discuss female safety. As a female Deliveroo rider it is really important to me that I can share my experiences with Deliveroo and personally get involved with Neighbourhood Watch in my local community."

Find out more here.

Cryptominer malware hidden inside online games

Avast Threat Labs report cracked versions of online games such as Grand Theft Auto V, Far Cry 5, and The Sims 4 that are laced with hidden malware - over 222,000 systems infected worldwide

Avast is warning gamers all over the world that they could be inadvertently helping cybercriminals make money by downloading illegal cracked games hidden with malware.

Versions of popular games such as Jurassic World Evolution, Grand Theft Auto V, and Pro Evolution Soccer 2018 are being given away for free in forums, however hidden inside these games is a piece of crypto-mining malware called Crackonosh, which secretly generates digital money once the game has been downloaded. So far, hackers have made over $2m (£1.4m) with the scam.

What does Crackonosh do?

When Crackonosh is installed, it automatically starts mining Monero crypto coins without the users' knowledge. It also takes actions to protect itself, including disabling Windows Updates and uninstalling all security software.
The crypto-miner programme, which then runs in the background, can slow down computers significantly, increase the users' electricity bills and put them at risk of security threats.

Which games are infected?

Crackonosh was found in the cracked versions of the following games:
NBA 2K19, Grand Theft Auto V, The Sims 4 Seasons, The Sims 4, Fallout 4 GOTY, Far Cry 5, Euro Truck Simulator 2, Jurassic World Evolution, Call of Cthulhu, Pro Evolution Soccer 2018, We Happy Few.

How to Avoid Crackonosh

The best way to protect against Crackonosh is to avoid it entirely by downloading games and other software only from official websites and stores.
Users are also advised to be aware of illegitimate sources offering paid-for games for free and to avoid unofficial vendors.

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.**

Warning about scam calls from "matching" mobile phone numbers

The National Fraud Intelligence Bureau (NFIB) is warning the public to be vigilant of scam calls that appear to be coming from numbers similar to their own **Read more**

How to spot Fake Reviews

Booking a holiday? Would you be able to spot a fake review? Check out **WhichUK** for their advice on misleading reviews, plus other useful tips to enjoy your #SummerSafety

Support if you have been scammed, guidance if you need it

Being scammed can have both financial and emotional detriment. Citzens Advice have put together a list of places where you can find support: **Read more**

citizens advice

Have you been misled or pressured into buying something? Check out CitizensAdvice for guidance **here**

Fraud trends and emerging issues

National Fraud Intelligence Bureau

TAKE FIVE TO STOP FRAUD™

The National Fraud Intelligence Bureau's (NFIB) monthly fraud update for May identified that Covid-19 vaccination scams, holiday fraud and job application fraud continue to be likely given the easing of travel restrictions and the impact of Covid-19 on the job market. In addition, new, emerging fraud threats have been identified to look out for:

• Action Fraud recently received 537 reports in 48 hours relating to **fake emails** purporting to be from British Gas. The emails state that the recipient is due a refund because of overpayment, and there is a link to a phishing website requesting personal and financial information. Do not be taken in by this – forward all scam emails to the Suspicious Email Reporting Service (SERS) report@phishing.gov.uk.

• Fraudsters have been using Covid-19 to solicit donations by impersonating legitimate charities. With the crisis in India being reported globally, it is likely fraudsters may use that situation and the reports of limited access to vaccinations in other poorer countries to scam members of the public wanting to help.

• A new **sextortion scam** has emerged in Canada where scammers are superimposing a victim's face onto a nude photo or a video of an individual engaging in sexual acts. The scammer threatens to send the image/ video to family or friends unless the victim pays money. Although the reports are based in Canada, we may see cases of this in the UK, and young people should be alerted to look out for and report any instances where they are targeted in this way.

• There has been a reported increase in the volume of young people suffering from **mental health problems** and a surge in the number being referred to mental health services due to the pandemic. We know through prior research that individuals with mental health issues are more likely to fall victim to scammers.

Fire & Rescue Service: Top Tip

London Fire Brigade has created a new tool called the Home Fire Safety Checker and it's designed to help people spot fire risks in their own home, or the home of anyone who they feel may be at risk.

The free tool asks a few simple questions about the household, and then guides the user around each room in the home pointing out which fire hazards to look out for. They're then provided with tailored advice and practical tips, which you can email to yourself or the homeowner to refer back to.

So please, check your own home, and then help a neighbour check theirs - you may well be surprised at what risks you've been overlooking for years. Click here to access the tool.

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 Crimestoppers: Report Crime Anonymously

CrimeStoppers.

0800 783 0137
100% anonymous. Always.

Speak up. Stay safe.

Money mules - what are they and could you fall victim?

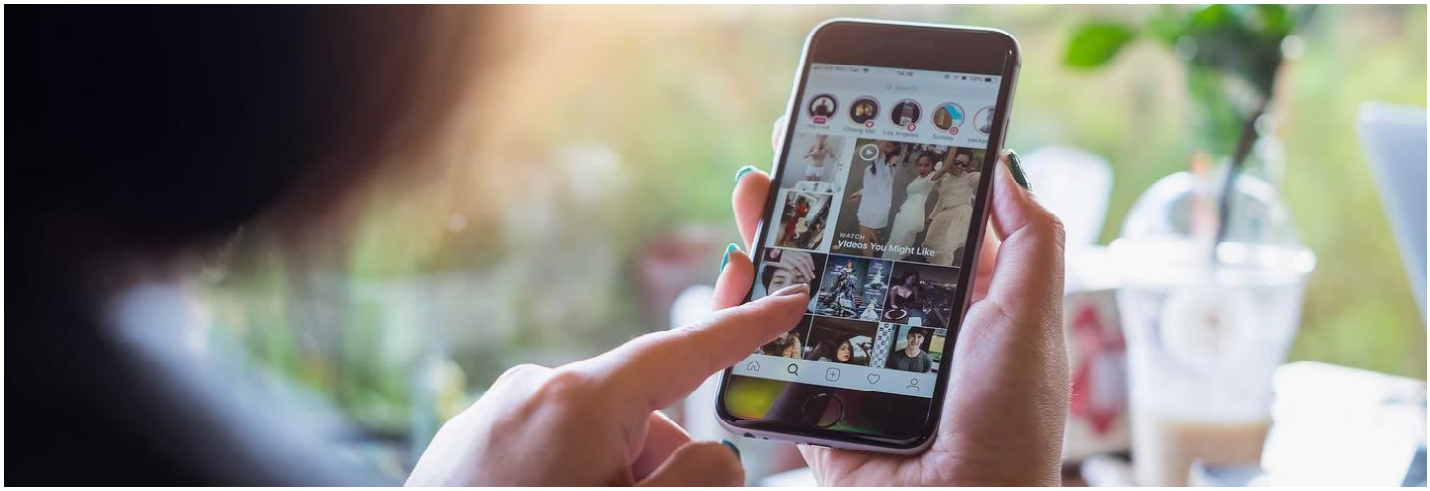
Criminals are targeting young people through Snapchat and Instagram promising that they can make hundreds of pounds in minutes by becoming a money mule.

Although it might appear to be a stress-free get rich quick scheme, acting as a money mule is illegal and could be funding serious crime, and make it hard for you to access credit in the future.

Crimestoppers has joined forces with TSB to educate young people on Money Mule scams - to help them stay suspicious of social media scams so they don't fall victim.

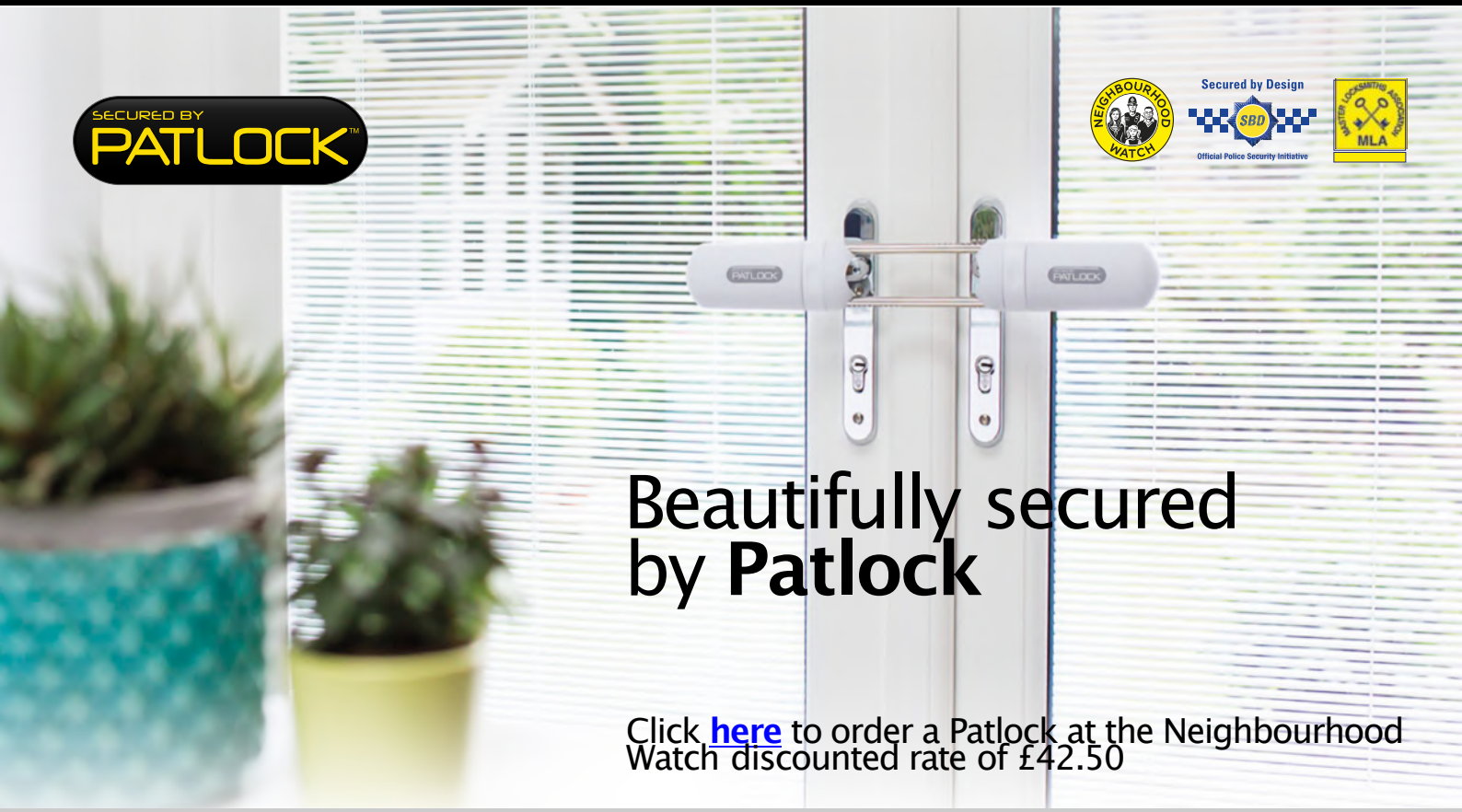
More details can be found on the Crimestoppers page **here**

The Money Advice Service organisation also offer advice and guidance on the website **here.**



Stay 100% anonymous. Always.

Neighbourhood Watch Benefits



SPECIAL 15%DISCOUNT FOR ALL NWN MEMBERS

Use Coupon Code NWNLock on Check Out.