



# Newsletter

> THE E-NEWSLETTER FOR NEIGHBOURHOOD WATCH SUPPORTERS IN SUFFOLK

**Welcome to the April edition of our newsletter.**

The executive team are busy getting plans in place for the forthcoming Annual General Meeting, which as like last year, will be held via an online process. Even though COVID restrictions are now starting to be lifted, we believe this is the safest and most sensible way to hold the meeting. It will also give all of our schemes the opportunity to take part and vote accordingly. More details will follow, and we will send out the first stage communication by 28<sup>th</sup> May 2021.

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:

NWN News **PG 2**

AVAST Fleeceware scams **PG 4**

Suffolk Crimestoppers **PG 6**

Which? free scam alert service **PG 3**

Suffolk Trading Standards **PG 5**

Action Fraud **PG 7**

## 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](mailto:comms@suffolknwa.co.uk)

Thank you to all the schemes that send us their newsletters. You can send yours to [comms@suffolknwa.co.uk](mailto:comms@suffolknwa.co.uk)

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



## Neighbourhood Watch Network: Campaign

Due to Covid-19 and repeated lockdowns, people haven't been using their cars as much as they used to. However, car crime remains a pressing problem in the UK – alarmingly, one car is stolen every ten minutes.

The latest figures from the Police National Computer indicate car crime decreased during Covid-19 controls, but with the expectation of social restrictions soon easing we could now see a surge in car crime.



The NWN have launched a new campaign to encourage everyone to keep their car's safety top of mind. Shockingly, 44% of cars are broken into through an unlocked door. 80% of car crime occurs during the evening or at night, and we all know that leaving valuables on display can attract car thieves.

So always remember to **LEAVE YOUR CAR: LOCKED, LIT AND EMPTY.**

**PROTECT YOUR CAR, LEAVE IT:**

- 1. LOCKED**  
LOCK YOUR CAR WHEN YOU LEAVE IT
- 2. LIT**  
PARK IN A WELL-LIT AREA
- 3. EMPTY**  
HIDE ANY ITEMS ON SHOW

**SHARE THESE 3 STEPS WITH 3 FRIENDS**

www.ourwatch.org.uk

Neighbourhood Watch Network is a charity registered in England & Wales. CID no: 1173249

## Neighbourhood Watch Network: Windrush Help Line

HM Government

# The Windrush Help Team

**Here to support you and your family**

Call **0800 678 1925** or visit **Gov.UK/WindrushHelpTeam**

Many people believe that the Windrush Help Line is only to help people who came to the UK from Jamaica on the ship Empire Windrush.

This is not true. The Help Line is there to help anyone who came to the UK from many other countries, including Nigeria, Ghana, Bangladesh and Pakistan.

Find out more [here](#).



## Neighbourhood Watch Week 2021: Don't forget!



5<sup>th</sup> -11<sup>th</sup> JUNE 2021



If the pandemic has taught us one thing, it is that neighbourliness and community spirit is just as important as ever, if not more so.

Neighbourhood Watch Week 2021 will be an opportunity for us to ensure that we build on the existing and new neighbourly relationships formed throughout the pandemic.

Whether we will be in lockdown or not, it'll be a time for us to celebrate and build on the connections we have made.

NWN are currently planning some exciting activities and building support materials which will be shared with us in the coming months.

**#LetsStayConnected**

### • Which? free scam alert service

# Which?

Unfortunately email, text, phone and social media scams are on the rise. People are falling victim

every day with scammers stealing billions of pounds. Which? is aiming to arm the public with the knowledge of how to spot and avoid scams.

Which?'s free scam alerts are regular email updates on the latest scams. They also include practical advice and next steps for victims.

If you are interested in signing up to Which?'s free Scam Alert service [click here](#).



## Fleeceware scams: Google Play and Apple App Store

**Fleeceware is a recently coined term that refers to mobile applications that come with excessive subscription fees.**

Avast's threat researchers discovered more than 200 new fleeceware applications on the Apple App Store and the Google PlayStore.

So far, the apps have been downloaded approximately one billion times and have accrued over \$400 million in revenue to date\*.

Avast has reported the fleeceware applications to both Apple and Google for review.

The applications attract users with the promise of a free 3-day trial, but once the trial is over, they are charged a recurring subscription fee - even if they deleted the app by that time - until they cancel the subscription in their device's app subscription settings. One of the apps, for example, offers a short free trial followed by a \$66 (£47.73) per week subscription, potentially costing the victim \$3,432 (£2,482.19) per year unless cancelled. These fleeceware applications are actively advertised on major social networks such as Facebook, Instagram, Snapchat and TikTok\*.

Avast's Threat Analyst, Jakub Vávra said "The fleeceware applications we've discovered consist predominantly of musical instrument apps, palm readers, image editors, camera filters, fortune tellers, QR code and PDF readers, and 'slime simulators'. While the applications generally fulfil their intended purpose, it is unlikely that a user would knowingly want to pay such a significant recurring fee for these applications, especially when there are cheaper or even free alternatives on the market."

"It appears that part of the fleeceware strategy is to target younger audiences through playful themes and catchy advertisements on popular social networks with promises of 'free installation' or 'free to download'. By the time parents notice the weekly payments, the fleeceware may have already extracted significant amounts of money."

Avast researchers discovered the Android fleeceware applications via its mobile threat intelligence platform [apklab.io](https://www.apklab.io), and then expanded their research to the Apple App Store.



### How to avoid Fleeceware apps

With subscriptions becoming more prevalent in app stores, people are encouraged to be vigilant when downloading and using applications. To avoid fleeceware, Avast has offered the following advice:

- **Be careful with free trials of less than a week**  
Applications that offer free trials for very short periods should be handled with caution. Make sure you understand how much you will be charged and that the app is worth the recurring fee.
- **Be sceptical of viral advertisements for apps**  
The advertisements for fleeceware are likely to have enticing messaging and images to attract users' attention. They likely do not reflect the actual functionality of the application.
- **Read the small print**  
A closer look will likely reveal the true price of the app. Read the application's details carefully, paying close attention to the 'In-app purchases' sections. Make sure to familiarize yourself with the conditions of what you're subscribing to, even if it is a free trial, as there may be automatic charges thereafter.
- **Secure your payments**  
Ensure that your payment methods are locked behind a password or biometric check. This can prevent accidental subscriptions by children as well.



# SUFFOLK TRADING STANDARDS



## Rogue Traders

There have been a number of reports across Suffolk recently where rogue traders have been operating.

In particular, three men in a white van have been seen approaching properties in the Lowestoft, Leiston and Eye areas, claiming that tiles are missing from roofs and needed repairs. Unfortunately, some residents have fallen victim, having paid money upfront for materials, but none of the "traders" have returned since.



If you, or someone you know have been approached, or perhaps you have seen them in the area, please contact Suffolk Trading Standards. Any details or descriptions of the individuals, as well as the vehicle will be invaluable.

Please share with friends, family and colleagues, as well as any community Facebook groups to help Trading Standards track them down.

Please report any information to us via 0808 223 1133, or online here: [Report to Trading Standards](#)

## "Cash for Jewellery" traders are leafleting in Suffolk

The best advice is to follow these simple tips to ensure you are getting the best deal.

**Shop Around** - No matter how or where you ultimately chose to sell, start locally. Contact a reputable local jeweller and ask them to estimate the value of your jewellery. That way, you'll at least have a base price in hand before you solicit online bids or other offers.

**Beware 'Rogue' Buyers** - Be wary of who you are selling your jewellery to! Are they a "rogue" buyer. If you have to leave your jewellery with them for a quote, do you know for sure that they will be there again when you return to collect your money?

**Read The Small Print** - Read the terms and conditions or small print, and pay attention to fees and charges that may apply. Refining fees, postage fees and appraisal fees could be hidden.



**Suffolk Crimestoppers: Report Crime Anonymously**

**CrimeStoppers.**

**0800 555 111**

100% anonymous. Always.

**Speak up. Stay safe.**

**Hare Coursing Alert**

**Speak up anonymously about blood sport crime**

**E**very year, crime in the countryside costs millions across the UK.

In 2019 rural crime cost the farming community £54 million according to the latest NFU Mutual crime report.

Hare coursing is a crime which has a significant cost to farmers. It is often linked to firearms and organised crime and endangers the safety of people living and working in the countryside.

### **Blood sport**

The illegal blood sport takes place in areas of open land where the dogs can easily pursue the hare. It is often carried out by large groups of people who travel long distances to meetings.

Such contests are live-streamed to allow more people to watch and bet, and often huge amounts of money changes hands for winning dogs. While hares are invariably killed, the dogs may also be injured during the chase.

Hare coursing involves poaching and trespassing with disruption and damage to fences and gates, caused by vehicles gaining access to private land and damaging fields and crops.

In countryside communities, people tend to know who's who. They may have information about this crime.

### **What you can do**

You should report any suspicious activity police on 999, particularly groups of people with dogs in multiple vehicles in isolated fields. Farmers who challenge hare coursers have been threatened with violence so, only if it is safe to do so:

- Take photos of or video the scene
- Note the registration of any vehicles, date, time, location and details of anyone involved.



If you hear of or suspect someone is involved in hare coursing or committing other crimes such as fly tipping, theft of livestock or quad bikes, but don't want to talk to police because you fear reprisals, then tell independent charity Crimestoppers what you know, **100% anonymously**.

### **Speak up and stay safe**

Crimestoppers won't ask for your name, or any personal details. We'll just listen to what you know and pass that anonymous information on to the police. Your call or online information can't be tracked or traced. You will be the only person who will know you contacted Crimestoppers.

**Crimestoppers is not the police.**

Contact us anytime on **0800 555 111** or online at **crimestoppers-uk.org**.

**It's 100% anonymous. Always.**

**No police. No witness statements. No courts.**



# Advance fee fraud

## FACTSHEET

### How does advance fee fraud work?

Advance fee fraud occurs when fraudsters ask victims to make advance or upfront payments for goods, services and/or financial gains that do not materialise. Fraudsters contact victims through mail, phone, email and social media.

### What can be done if you are a victim?

If you paid via bank transfer or money transfer, consumer rights organisation Which? Explains how you might be able to get your money back after you have been scammed.

[www.which.co.uk/consumer-rights/advice/how-to-get-your-money-back-after-a-scam](http://www.which.co.uk/consumer-rights/advice/how-to-get-your-money-back-after-a-scam).

Action Fraud cannot help you recover any money lost to fraud.

### Some examples of advance fee fraud include:

- You've won a cash prize or a lottery jackpot and, in order to claim the money, you must send a payment as a release fee in order for you to receive your prize.
- You've struck up a relationship with someone online and they invent a reason to ask for cash, using the emotional attachment you've built with them to get you to send money.
- You are a would-be tenant and are tricked into paying an upfront fee to rent a property that doesn't exist.
- You are contacted by someone who says they are from the HM Revenue & Customs (HMRC) and you are owed a tax rebate, but you have to pay a fee in order to receive it.



### Reporting to Action Fraud

Reporting to Action Fraud enables intelligence to be gathered and preventative action to be taken by police. For example, suspending websites used to commit fraud.

It is difficult for police to investigate every instance of fraud – prevention and protection is a far better method of dealing with it. By taking some simple steps, you can avoid falling victim in the future.

In some cases, the police and other law enforcement agencies may want to contact you for further details so it is important that you keep any relevant information about the crime.

## Action Fraud

National Fraud & Cyber Crime Reporting Centre

[actionfraud.police.uk](http://actionfraud.police.uk)

