Issue 7

LOCAL WATCH-WORD

The Newsletter of the Eastleigh Neighbourhood Watch Association keeping you up to date with crime and safety issues in your area

Sep 2021

Driving with E's (New Fuel Type)

Starting in September, standard petrol at garage pumps will change. The new petrol will be marked as 'E10' (note diesel fuel will not be changing). This is part of moves by the government to reduce carbon emissions.

Most cars built since 2011 will be compatible with this revised fuel. If your petrol car was built before 2011, or you ride a motorcycle, you can use the online vehicle checker at www.gov.uk/check-vehicle-e10-petrol to see if your vehicle can use this fuel. Alternatively, check your vehicle handbook.

Some other petrol-powered equipment may not be compatible with E10 petrol including boats, garden equipment such as lawnmowers and chainsaws and some light aircraft. Owners and operators should check their manual or ask the manufacturer or dealer before using E10. If in doubt, continue to use the E5 (super) grade.

If your vehicle or equipment is not compatible with E10 fuel, you will still be able to fill up with 'super' grade petrol from most filling stations - at least for the next five years.

So what if you make a mistake at the pumps and fill your older car with E10? Well, unlike the consequences of a petrol-diesel mis-fuel, expensive draining of the fuel system is not required. Simply dilute it with E5 from then on or fill it up next time with 'super' and it should be fine. 'But don't make a habit of it', say the manufacturers. Prolonged use of the wrong fuel could result in problems such as finding the engine harder to start from cold, stalling, leaks and corrosion.

Inevitably scammers will try to take advantage of the change to convince owners of non-compatible cars to hand over cash e.g. charging for unnecessary services such as cleaning out your fuel system. Please be prepared for the change and, if you fuel up wrongly and use the incorrect fuel for your vehicle, don't panic - just dilute with E5 and go over to using this as soon as possible.

Quarterly Tip

If a thief stole pages from a dictionary

Would it just go from Bad *to* Worse!

Deliveroo Bringing More Than Just Food

Neighbourhood Watch announced our partnership with Deliveroo during Neighbourhood Watch Week. The vast majority of feedback has been very positive. Association Leads and members say that having Deliveroo riders as additional eyes and ears in our communities can only be a good thing.

We will continue to work with Deliveroo and their riders to ensure they can opt-in to receive training in personal and community safety and are seen as a positive part of the communities in which they live and work.

CONTENTS

A Note From Our Chairman

Mike Anthony

Holidays are here at last! Many of us are ‘staycationing’ in the UK this year. Indeed, judging by the roads, the New Forest is very busy this summer (despite the indifferent August weather). The latest edition of Rural Times is now available (go to https://www.hampshire.police.uk/SysSiteAssets/media/downloads/hampshire/advice/rural-times/rural-times-august-2021.pdf). Without being overly negative, one of the articles talks about what to do if you come across an injured deer or collide with a deer (or other animal) in the New Forest. When reporting an incident, give as precise a location as you can - a good tip (for any emergency call) is to use the smartphone App *What3Words*. This enables you to define where you are to and accuracy of 3 metres.

Please remember to take your waste home with you. If you come across any fly tipping, report it using the website link given on page 3.

Back home, the best way to allow police visibility of our NW schemes and contact details for coordinators (or deputies) in the event of an incident, is to have all coordinators registered on Alert. The easiest way is probably via the OurWatch website which also allows you to map your scheme. We presently have just over 69% of coordinators registered on Alert - I would like this to be much higher, so please take a few minutes to do this. If you have trouble please speak to your Area Coordinator or contact me and we’ll assist you.

Lots more information can be found on our ENWA website

www.eastleighnhw.org.uk/

and also
take a look at
our Facebook page

Ad Hoc Tic Toc Block

TikTok is an app that is especially popular with young people as it provides opportunities to create and share short-form videos.

TikTok runs on both Apple and Android phones and tablets and has selected a 12+ rating on the Apple App Store and Google Play so that parents can use the device-level parental controls provided by Apple and Android.

For example, parents can restrict what content can be downloaded or purchased from Google Play based on maturity level. To do this, go to Google Play on your child's Android device and **navigate to Menu > Settings > Parental Controls**.

TikTok has several educational resources for parents including a Top Ten Tips for Parents primer, “You’re in Control” (go to tiktok.com). For a parents guide to TikTok go to https://www.connectsafely.org/tiktok/

Banking Scam Calls

If you get a call from someone claiming to be your bank or the police and they ask you to transfer money to another ‘secure’ account, hang up - it’s not your bank or the police.

It’s also easy for scammers to spoof legitimate phone numbers using software shared by criminals freely online. So just because your Caller ID says it is your bank it may not be. **Put the phone down and check by calling your bank on a number you have (not one the caller gives you).**

Watching Your Waste-line

You are responsible for your waste.

With fly-tipping becoming a major problem for councils, they are taking steps to trace the originator of the waste. Even though you may not have been directly involved in the fly-tipping if it can be proved that the waste was originally yours, you may still be liable to prosecution.

How do I avoid a fine?

It is your duty of care to dispose of your waste correctly. You could be fined an unlimited amount by your local council if your waste ends up fly-tipped, and you cannot show that you took reasonable steps to prevent it.
If convicted at court, the maximum fine is unlimited and you could face 5 years in prison.

You must use a licensed waste carrier, or take your waste to a registered site.

Check if your waste carrier is licensed
Check their waste carrier licence number on the Environment Agency register of waste carriers.
Ask what will happen to your waste - a licensed waste carrier should not object to reasonable questions.
Make sure you get a waste transfer note and receipt for your waste and keep it as proof.

Take your waste to a registered site

There are 26 household waste recycling centres in Hampshire. They are open 7 days a week except Christmas Day, Boxing Day and New Year's Day.

Most waste is free to dispose of.
There are charges for householders taking soil and rubble (£3 per standard rubble sack or item of sanitary ware and plasterboard (£10 per sheet / £6 per bag).

Collection of bulky waste by local councils:

Most councils will collect things like old sofas, fridges or washing machines for a fee.

For more information see:https://www.hants.gov.uk/fly-tipping

‘Ware’ Jargon Buster

Malware:

Malware is an umbrella term for any type of “malicious software” that’s designed to infiltrate your device without your knowledge.

There are many types of malware, and each works differently in pursuit of its goals. However, all malware variants share two defining traits: they’re sneaky, and they’re actively working against your best interests.

No matter the type, all malware follows the same basic pattern: The user unwittingly downloads or installs the malware, which infects the device.

Ransomware:

Ransomware is a type of malware, or malicious software, that takes files — and sometimes entire computers or mobile devices — hostage. We can define ransomware by this behaviour,: hackers will request a ransom payment in exchange for returning access, or decrypting your files.

You’ll know immediately if you have ransomware, as it cuts off access to your infected device and usually encrypts your files. In both cases, you can no longer open and work with vital data, such as work documents and personal photos and videos. The cybercriminals behind the attack will contact you with their demands, promising to unlock your computer or decrypt your files once you’ve paid the ransom

Spyware:

Spyware is a type of malware that tries to keep itself hidden while it secretly records information and tracks your online activities on your computers or mobile devices. It can monitor and copy everything you enter, upload, download, and store. Some strains of spyware are also capable of activating cameras and microphones to watch and listen to you undetected.

Once it’s on your computer or mobile device, spyware can carry out a distressing array of covert operations, including:

- Keylogging (recording everything you type, including usernames, passwords, banking info, etc.)
- Recording audio and video, and screenshot capture
- Remote control of the device
- Capturing content from email, messaging, and social apps
- Recording and capturing browser history

Adware:

Have you ever been browsing the internet, going about your day, when suddenly you get inundated with messages? If you assumed they were probably spam, you’re right! If you’re seeing a ton of ads like this, you probably have a particular type of malicious software, called adware, on your system. To define adware is simple: it is software that hijacks your browser or other parts of your system in order to blast you with unwanted ads.

Adware exists to generate revenue for its owner, who earns money every time you click on one of the ads they’ve shown you. As adware tracks your web browsing, it can present targeted ads linked to your interests. It can also sell your browsing history to third parties. And it won’t stop if you switch browsers — adware lives on your operating system itself, and so no matter which app you use to browse, the ads will be there.

The internet can sometimes feel like a battlefield teeming with malware, but everyone should be able to browse safely and confidently. A strong antivirus program acts as a moat that surrounds and protects your cyber-castle. Download a trusted antivirus programme to stay completely safe online.

Police & NW meet the public

On Saturday 21st of August, the Fryern Arcade in Chandler's Ford was the venue for an opportunity for the residents of the Chandler's Ford and Hiltingbury area to put questions to local PCSOs Victoria and Andy and Neighbourhood Watch representatives John, Claire and Pauline. John and Claire are both Cyber-Champions and are able to offer practical advice on dealing with scams and other cyber-crimes. This FREE service can be accessed through the Hampshire Cyber Watch website: https://hampshirecyberwatch.org/

PCSO Tor (Victoria Amery) said:

Today's Beat Surgery was a success.

We delivered and handed out lots of crime prevention advice. We also squeezed in 4 Blue Lamp Trust referrals.

Thank you very much to the wonderful Neighbourhood Watch team who came out to join us, To The Flower Shop for allowing us to use their store front, and of course to the people of Chandlers Ford and Hiltingbury who came and spoke to us.

We gave out countless stickers and colouring pictures to the children who came over for a chat, we do hope that you'll share your coloured in poster with us by tagging us using #eastleighpolice

Once again, thank you for a great morning.

PCSO Tor

How Smart is your Home?

Because many new smart devices for the home connect to the internet, it's not only your computer that is vulnerable to attack by malicious hackers. Door cameras, Wi-Fi printers, smart speakers and even kettles can be targets. In a recent test conducted by 'Which' they detected thousands of attempts to hack into their simulated 'smart home'.

There are, however, some simple steps you can take that will vastly improve your connected home security.

- Change default passwords: A weak default password is the easiest way for a device to get hacked. Always change any password that comes with the product you buy or already own.
- Enable all security: Take some time to see what security features are available in the manual or app settings. If two-factor authentication is available, use it as it can better protect your account.
- Run updates: Always install any security updates for the product or app so you've got the most recent protections. Under the new law, manufacturers must tell you how long your product will be supported with such updates when you buy it.
- Be wary of phishing: Some smart devices can be remotely exploited simply with a phishing message, enabling a hacker to fully compromise the device. So, always stay vigilant to any phishing messages sent to you via text or email.
- Take it back: If you believe a smart product you own is insecure, you could try returning it to the retailer for a refund.

WhatsUpp WhatsApp

A scam which steals your identity and WhatsApp account is a problem that has recently been identified. The first indication of this may be an unexpected genuine message from WhatsApp with a verification code. Following this you get a message, apparently from a friend, asking for the code. Because it seems to be from someone you know, your guard is down. The hacker has already got control of their account and if you send them the code they will, in turn, have control of your account.

Once in control they can kick you out of your own account, access your contact list and messages and go on to carry out the same scam on others on your list. By pretending to be you they may be able to persuade contacts to send them money or information that could compromise bank accounts etc.

So, to avoid this happening to you:

- Don't share your login details or verification code with anybody. Not even your closest family or trusted friends.
- Set up two-step verification to secure your account.
- Be wary of WhatsApp messages requesting money, even if they come from your contacts. If you're not sure, give the friend a quick call to check.
- As always, if you think you may have given sensitive details, such as payment information, to fraudsters, let your bank know what's happened immediately.