Adur NHW Newsletter

Shoreham & Southwick Issue

March 2025

Your Committee

David Hansford :	Chair
Doris Martin	Deputy Chair
Steve Male	Secretary
Steve Martin	Treasurer
Ron Marsh	Committee Member
Robin Monk	Committee Member
John Nutt	Committee Member

Email: adurnhw@gmail.com

Electricity Theft

Have you noticed that your electricity usage has significantly increased lately and you have ruled out any likely explanation for that? Then there's a chance that someone could be stealing your electricity.

Electricity theft involves someone intentionally stealing electricity - or paying less than they should by tampering with or bypassing their own meter - and is a crime punishable by a fine of up to five years in prison. It is estimated that energy theft is costing UK energy suppliers around £440 million a year and inevitably those costs get passed on to consumers.

Electricity theft is not just a financial issue, it's also dangerous. It can cause injury and in severe cases, even death. That is because electricity theft often leaves wires exposed, which can cause fatal electric shocks, start fires and even trigger explosions.

With that in mind, investigating potential electricity theft in your own home should be approached with extreme caution. In fact, it is far better to let the authorities deal with it instead.

If theft of electricity is indeed to blame for a high electricity bill, there will often be other clues. Signs that someone is stealing your electricity may include:

- Changes to your wiring – take a look at the wire that runs between your meter and your house (but don't touch it!). If you notice anything odd, like extra wires or connector clips, there's a chance that someone's tampered with it. Also, be on the look-out for any wires connecting your home to your neighbour's.
- Damage to your meter – look out for things like scorch or burn marks, a burning smell, loose or strange wiring, or even sparks. This is a strong indication that your meter has been tampered with.
- Your meter acting strangely – if your meter keeps running even after you switch off your circuit breakers, it's an indication that something is taking power from between the electric panel and the meter itself. If the numbers on the dial are moving the wrong way, or not at all, this could be a sign of a tampered electric meter.

Artificial Intelligence

Cyber criminal tactics are on the rise and this year, with AI-driven scams becoming much more insidious. Cyber criminals are making it ever more difficult to differentiate between genuine and fake, and AI will empower them to raise the threat that they pose significantly.
There are six AI scam predictions for 2025 of which every Internet user needs to beware:

- Using AI, scammers are developing more sophisticated attacks (including phishing emails, malicious links, and scam texts) which can be visually undetectable, so it's crucial to use advanced technology to detect scams.
- Generative AI is enabling highly personalised phishing attacks on an unprecedented scale. Scammers can now use AI to conduct tech or customer support scams, but make them look more authentic. Now thousands of AI assisted calls can be tailored, the more easily to deceive the victim – aided by a real human voice, real answers, and relevant responses.
- Every data leak or personal detail you share online will be used against you. Scammers can tailor phishing messages, emails, and calls with specific personal data on each victim, thus heightening the danger that they pose. Beware of what you share - it could be weaponized against you.
- Generative AI enables scammers (even those without design skills or knowledge of the target language) to produce professional-looking images and messaging, and tactics can rapidly be updated so as to avoid detection. This can be used for everything from package delivery scam texts to fake shopping websites.
- Scammers will increasingly target AI tools like ChatGPT, which store vast amounts of personal data. Your genAI account logs every piece of information you input and every question you ask - work-related information, personal details, and even sensitive intellectual property. Scammers can access this data, exploiting your AI assistant to retrieve critical information.
- Fake generative AI sites are mimicking OpenAI, reflecting growing user interest and increased ad targeting by businesses - and potentially by scammers. As fraudsters tend to follow popular trends, a rise in malicious websites disguised as AI-related services and designed to distribute malware is expected.

Pegasus Card Scheme

For those who, through disability such as speech impairment or loss of hearing, find it hard to communicate with the Police during an emergency or difficult situation, the Police have a scheme - "Pegasus" - aimed at breaking down this barrier. It was developed by Chris Channon MBE, a former paralympian who suffers from cerebral palsy.
Registration is free and open to anyone who fits the above criteria, as long as it is done with the Police force in your neighbourhood.
Once registered, you will be issued with a card and a personal identification number (PIN) and if you need to call the Police, say 'Pegasus', tell them your PIN and they can then access your details immediately. You can also show your card to a Police officer, member of Police staff or other emergency services staff if you need assistance in person, and then they'll know that you may need extra help and support.

If you agree, the Police will share your information with other participating emergency services (fire, ambulance) and local authorities. You can change or update your details at any time.

Your information will be stored on a secure database owned by the Police. Access to this database is controlled, but the Police may share your details with other emergency services, so that they can help you. You must have your parent or guardian's consent if you are aged under 18.

On registration, you will be asked for:

- your contact details
- information about your disability or impairment, and how it affects your day-to-day life
- details of up to two trusted people that the Police can contact if they can't get hold of you

This process saves the caller valuable time which would have been spent trying to give personal details, and should go a long way towards bolstering the confidence of those for whose benefit the system was devised. The information also improves Police ability to understand any communication barriers there may be, and to provide assistance accordingly.

A Hard-hitting campaign has been launched to help tackle the growing problem of drivers using their mobile phone behind the wheel.

The campaign, launched by East Sussex County Council, West Sussex County Council and Brighton & Hove City Council, highlights the serious consequences of using a phone whilst driving with the strapline 'one second of distraction, a lifetime of regret'.

It follows an increase in the number of drivers admitting to using their phone behind the wheel and one in five drivers aged 17-24 confessing to taking part in video calls whilst driving.

The message will be shared across Sussex with campaign posters on buses and at petrol stations, adverts on local radio and posts on Snapchat, Youtube, Facebook and Instagram.

Cllr Claire Dowling, East Sussex County Council's lead member for transport and environment said: "The increase in drivers who admit to regularly using their phone behind the wheel is extremely worrying.

"Some drivers underestimate the dangers of using a phone whilst driving, even a split-second lapse in concentration whilst changing a song on a playlist or checking a text message can have serious consequences.

"We hope the campaign will highlight those dangers and make people think twice about picking up their phone."

Motorists are four times more likely to crash when using a phone, and more than half of drivers admit that mobile phones are their biggest distraction whilst driving.

The Sussex-wide campaign urges drivers to pledge not to use their phone behind the wheel by visiting https://eastsussex.gov.uk//RoadPledge

Cllr Joy Dennis, West Sussex County Council's Cabinet Member for Highways and Transport, said: "We work hard to make Sussex's roads as safe as possible for all who use them, but we rely on drivers to do their part. It only takes a short break in concentration on the road ahead for a collision to occur, sometimes with life changing impacts.

"As tempting as it may be to quickly read a text or clear a notification, it's not worth the risk so we strongly hope that this campaign will encourage drivers to ignore their phones and give their full attention to their surroundings, keeping them and all other road users safe."

Cllr Trevor Muten, Brighton & Hove City Council's Cabinet member for Transport, Parking and Public Realm added: "We've all seen the devastating and life-long consequences using a phone at the wheel can have.

"I hope this campaign will make people really think about their actions. Even the slightest distraction can be deadly."

As well as increasing the risk of crashing by up to four times, using a mobile phone while driving is illegal and can result in a fine of up to £1,000, six penalty points, and a driving ban.

More information about the campaign and advice on how to stay safe is available at https://eastsussex.gov.uk//RoadPledge

Crime Statistics for January 2025

Police UK have not produced the January 2025 results at the time of going to press

Home security doesn’t just mean locking your doors and windows – protecting your digital devices with strong passwords is also important to keeping yourself and your personal data safe. And creating a strong password is not a complicated procedure; you can protect your devices and digital data by taking just three simple steps.

First, create a separate, strong and unique password for your personal email account. Your personal

email account contains lots of important information about you and is the gateway to all your other online accounts, including banking, social media and online shopping. Remember that weak passwords can be hacked in seconds.

Second, the recommended method of generating passwords is to use three random words, as it’s easier to remember and takes trillions of years for a computer algorithm to crack. The Cyber Resilience Centre (a not-for-profit organisation, owned by the police, that works across the UK in partnership with industry, government, academia and law enforcement) recommends looking around a room and picking out three of the objects there. Thus, for example, table, computer, map would become tablecomputermap – never use words that are associated with you, such as the names of pets or surnames, as these are easy to identify if you are someone who uses social media.

Having used this formula to create your email password, repeat the process with your most important accounts, such as banking and social media, and replace your old passwords with new ones.

And third, make use of two-factor authentication (2FA), which is a free security feature that gives you an extra layer of protection online and stops cyber criminals getting into your accounts - even if they have your password. 2FA reduces the risk of being hacked by asking you to provide a second factor of information, such as getting a text or code when you log in, to check you are who you say you are. So check whether the online services and apps you use offer 2FA – it’s also called two-step verification or multi-factor authentication – and be sure to make use of it if it is available.

See the latest Alerts at : https:// worthingnhw.ourwatch.org.uk/