Issue 26

LOCAL WATCH-WORD

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

Jun 2026

DO'S AND DON'TS OF SOCIAL MEDIA

Do's

- Adjust privacy settings: Set your profile to "Friends" or "Private" so only approved contacts can see your posts and information. Learn how to manage who can find and contact you.
- Use strong passwords: Create unique, long passwords with a mix of letters, numbers, and symbols. Consider using a password manager for added security.
- Be selective with connections: Only accept friend requests from people you know and trust in real life. If a friend sends a second request, verify it with them offline first, as their account might be duplicated by a scammer.
- Verify information before sharing: Check the credibility of sources before believing or sharing news. Reliable news outlets and official government accounts usually have a verified checkmark.
- Ask for help: Don't hesitate to reach out to tech-savvy friends, family, or community groups, for guidance. You can also find many step-by-step tutorials online.

Don'ts

- Don't overshare personal details: Never post your home address, phone number, financial information. Avoid revealing you are on holiday, as this could signal your home is empty.
- Don't accept requests from strangers: Be wary of friend requests or messages from people you don't know, especially if they quickly ask for personal information or money.
- Don't click on unknown links: Be cautious of unsolicited messages, advertisements, or emails that contain links, even if they seem to come from a friend or your bank (verify first).
- Don't believe everything you read: Misinformation and fake stories spread easily. If something seems too good to be true or designed to provoke an emotional reaction, it likely is.
- Don't use easily guessable usernames/passwords: Avoid using your name and birthdate. Choose secure, non-personal details.
- Don't post pictures of others without permission: It is good social etiquette to ask friends and family if it is okay to post their photos online before you do.

Quarterly Tip

Verify the sender and hover over links before opening them.

CONTENTS

A NOTE FROM OUR CHAIR

Claire Wills

Not a lot has happened over the past 3 months as I have been out of action – just getting back into things but sitting for long at a computer is not good! We have been unable to attend fetes etc this year, since many councils are now farming out all the organisation of the events to a company and we have been informed that we need a commercial quality gazebo and solid weights to hold it down. We are hoping to get a grant from one of the councils to fund this so that next year we will again be visible at such events.

Our AGM will be held on Tuesday 7th July at Boorley Green Sports Pavillion at 7:30pm– more information will be sent out nearer the time. We are hoping to have a good speaker – just waiting for confirmation of their availability.

I have been informed (and am following up) a situation where some incidents did not appear on the Incident Reports list published on the website. If you know of any incidents that were reported but do not appear, could you please let me know. We need to have confidence that all those things that are reported show up and are acted on.

A reminder for any of you who organise events in your area, either for your members or to promote Neighbourhood Watch, that you can be covered under Neighbourhood Watch Insurance – just let me have details and I can confirm cover.

Thanks again to all members and coordinators for their support.

Claire

WWW

Lots more information can be found on our ENWA website

www.eastleighnhw.org.uk/

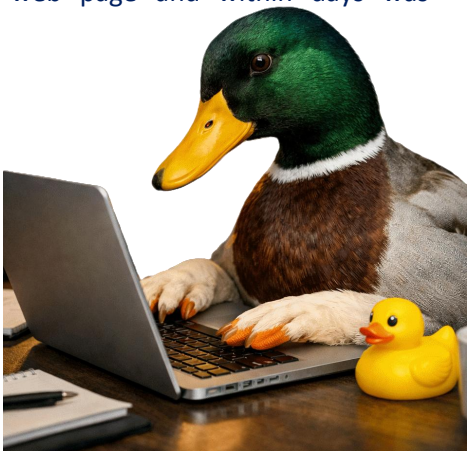
and also take a look at our Facebook page

CORBEN'S CORNER

By John Corben

Who remembers the saying 'if it looks like a duck, walks like a duck and quacks like a duck then it must be a duck' ...well, with the advancement of Artificial Intelligence (AI), and how it is impacting on computer hacking, this is no longer true. Whilst AI has the potential for great good, it can also be used for great deception as well. It can mimic exactly a company web pages, which could be almost impossible to tell apart from the real page. It can also mimic people visually and their voice to the extent that the 'fake' AI image is almost impossible to tell from the real person. Indeed, I have heard reports that scammers can 'scrape' a person's voice pattern from their answerphone message and with manipulation mimic almost perfectly their voice. Now this is all getting scary and increases the need for even more vigilance. So nowadays if it looks, walks and quacks like a duck ..... it might now be a scammer.

Data brokers buy and sell information. This information may well be personal information about us, passed to them by a company we have an account with. This passed on data may include our name, our email address, our phone number and possibly our address. This data could well be in the public domain, as a result of a cookie we have agreed to being downloaded onto our computer, or as a result of visiting a company web page in order to browse or make a purchase. If the cookie settings are not checked fully and amended as below, we may well be accidentally allowing that company to pass or sell our data to third parties. If possible, reject cookies or at the very least restrict which cookies are allowed. As a rule of thumb, if cookies can't be rejected, restrict them to essential use only by changing preferences before confirming. I made the mistake once (in my opinion) of seeing how much my car was worth on the second-hand market. I duly entered my details on the company web page and within days was inundated by dozens of emails, some I believe of questionable origin. Coincidence? I am still not sure.



Data about us can also be obtained by hackers from the Dark Web. This could be as a result of a company being hacked and any resulting information being sold on in packets of, for example, 10.000 sets of personal information to another scammer for a fee of, let's say, £50.00. This personal information is generally in plain text, not encrypted, and allows the scammer, assisted by an AI generated email or SMS message to personalise an attack against their intended victim. I had one of these email messages only a few weeks ago, purporting to be from my bank. The message was an exact replica of emails I had received previously from my bank, text, font, colour and layout and referenced a recently introduced piece of financial legislation. The only problem was, it was a scam email and it was attempting to get me to update my personal information by clicking on a link. Needless to say, I reported the email to report@phishing.gov.uk, blocked the sender and deleted the email. Contacting the bank confirmed this was a scam email.

Please remember - the duck may not be all it seems.

THE DIGITAL DILEMMA: KEEPING CHILDREN SAFE ONLINE

Keeping children safe in a fast-moving digital world has become one of the biggest challenges for parents and carers. With smartphones, gaming, social media and AI-driven scams now part of everyday life, understanding the risks — and the protections available — is essential.

The **National Cyber Security Centre (NCSC)** provides clear guidance on safe social media use, strong passwords and spotting suspicious activity. Tools such as **Police CyberCheck** allow families to quickly assess whether a website, message or online offer is genuine. Parents can also check whether their email has appeared in a data breach using **Have I Been Pwned**, a simple but powerful early-warning tool.

AI voice-cloning has emerged as a new threat, with scammers able to replicate a voice from as little as **eight seconds** of audio. Teaching children and relatives to use **safe phrases** — agreed code words that must be used in emergencies — can prevent manipulation.

Practical device controls remain vital. **Internet Matters** offers step-by-step guides for Apple and Android parental controls, e-safety checklists, and advice on setting up child-friendly Google accounts. Platforms such as **Snapchat Family Centre** and **TikTok Family Pairing** give parents visibility over who children interact with and allow location settings to be switched off.

Financial safety matters too. Banks such as **NatWest**, in partnership with Cifas, highlight how easily personal information can be exposed and misused. Teen banking accounts now include built-in protections to help young people learn safe digital habits.

For younger users, gaming guidance from **Ask About Games**, online-safety support from **CEOP**, and resources from the **UK Safer Internet Centre** help families navigate risks ranging from inappropriate content to grooming and DDoS-related attacks on home routers.

The digital world offers huge opportunities — but staying informed, setting boundaries and using trusted tools ensures children can explore it safely and confidently.

ANOTHER COOKIE WITH YOUR COFFEE?

Cookies are small pieces of data that websites store in your browser to remember information such as logins, shopping baskets and preferences. They are tiny text files sent back to the website each time you visit so it can recognise your device and track activity.

What cookies are used for:

- **Session management** – keeping you logged in or maintaining your basket
- **Personalisation** – saving language, layout, or theme settings
- **Tracking** – analysing browsing behaviour, mainly for advertising (third-party cookies)

Types of cookies:
- **Session cookies** – temporary; deleted when the browser closes
- **Persistent cookies** – remain until they expire or are deleted
- **First-party cookies** – set by the site you're visiting
- **Third-party cookies** – set by advertisers for cross-site tracking

Cookies can store sensitive data like login tokens. While most are harmless, tracking cookies can build detailed profiles of your browsing habits, which is why GDPR requires websites to ask for consent.

Should you accept cookies?
You don't need to reject all cookies, but you *should* reject unnecessary ones.
- **Accept essential/necessary cookies** – required for the site to function

Reject marketing, advertising, analytics, and personalisation cookies unless you want them. Accepting cookies can make sense if you want a site to remember your login or preferences.

Deleting cookies:

It's safe to delete all cookies, but it will log you out of websites and reset saved settings. Clearing cookies improves privacy, removes tracking data, and can fix website issues. Most people only need to do this occasionally.

How to delete cookies (Chrome example, very similar with other browsers):

Settings → Privacy and security → Clear browsing data → Tick *Cookies and other site data* → Clear data.

DON'T LOSE YOUR BICYCLE

With some bicycles costing over £1000 they are increasingly becoming targets for thieves. Even if your bike is of negligible financial value, having it stolen could well be a frustration, leaving you stranded.

Keeping your bicycle secure requires a mix of good equipment, smart habits, and a bit of awareness. Start with a **high-quality D-lock** made from hardened steel. Cheap locks can be cut in seconds, so investing in a Sold Secure Gold or Diamond-rated lock dramatically improves your chances of keeping your bike safe. Pair this with a **secondary lock**, such as a thick cable or chain, to secure removable parts like wheels or the seat post.

Always lock your bike to a **fixed, immovable object**—a metal stand, rail, or ground anchor. Avoid thin posts or anything a thief could lift the bike over. Position the lock so it passes through the **frame and the rear wheel**, filling as much space inside the D-lock as possible. This reduces leverage points for tools. Keep the lock off the ground, as this makes it harder to smash.

Choose your parking spot wisely. Well-lit, busy areas deter thieves far more than quiet corners. If you're leaving your bike for long periods, use designated cycle parking or monitored locations whenever possible. At home, don't rely on a shed alone—fit a **ground or wall anchor** and lock the bike inside. Many thefts happen from gardens and garages, so treat home storage as seriously as public parking.

Remove accessories like lights, GPS units, or quick-release saddles. Thieves often take what's easiest. Mark your bike with a **police-approved security marking kit** and register it on a national database. This helps recovery if the worst happens.

Finally, vary your routine. Parking in the same spot every day makes your bike a predictable target. A few small changes can make a big difference in keeping your bicycle safe.

UP AND OVER CAN BE MORE LIKE IN AND OUT

There have recently been several garage burglaries. Whilst these may be isolated incidents, you may wish to consider some of the advice below concerned with improving up and over garage door security:

Fit **additional garage door locks**

Most up-and-over doors only have a single centre lock, which is easy to attack. Adding extra locks makes a big difference.

Good options:

- **Ground anchor + locking bar** (very strong)
- **Side-bolt locks** that secure the door to the frame
- **Hasp and staple padlock system** (simple but effective)

These create multiple locking points, making the door far harder to force.

Reinforce the **internal locking mechanism**

If your door has a T-handle lock, the internal rods can sometimes be bent or pushed aside.

You can improve this by:

- Adding **steel plates** behind the lock
- Upgrading to a **high-security euro-cylinder**
- Installing **locking rod shields**

This stops intruders manipulating the lock from outside.

Secure any **windows** in or near the garage

If your garage has windows, they're often the weakest point.

Strengthen them with:

- Laminated security film
- Window bars or grilles
- Opaque film to stop people seeing inside

Improve **lighting and visibility**

A well-lit garage is a far less attractive target.

Consider:

- Motion-activated LED floodlights
- A dusk-to-dawn light above the garage
- Smart lighting that triggers when you arrive home

Add a **camera or smart sensor**

Even a basic camera or door sensor acts as a deterrent.

- A Wi-Fi camera pointing at the garage
- A smart contact sensor that alerts you if the door opens
- A driveway camera covering the approach

Strengthen the **garage door itself**

If the door is older or thin, you can stiffen it with:

- Steel bracing bars
- Cross-bracing kits
- A full door upgrade if it's very old

Modern up-and-over doors are much more secure than older ones.

A **physical barrier** can also make access to the door more difficult.

Consider reversing your car hard up against the door to protect both the garage door and also any contents of the car boot. Obviously valuable items should not be left in cars overnight.