Neighbourhood Watch Cyber Security Meeting

24th February 2026 – Martlesham Parish Room

We would like to thank everyone who joined us last Tuesday for our Neighbourhood Watch Cyber Security session at the Parish Room.

Guest Speaker: Gemma Theobald, Suffolk Constabulary

We were pleased to welcome Gemma Theobald, Cyber Security Advisor for Suffolk Constabulary, who provided an informative presentation on improving cyber awareness and staying safe online.

Gemma began with a short self-assessment quiz, where most attendees rated their cyber awareness as average. She highlighted that cyber crime continues to increase, with around 95% of incidents stemming from human error.

Digital Footprints

The majority of people have a digital footprint trail, and these trails can be defined as either **active** or **passive**.

- **Active Footprints**: Information shared intentionally, such as social media posts, accepting cookies, online forms and search engines.
- **Passive Footprints**: Information collected without direct control, including social media posts from friends and family, tagging and data breaches.

Social Engineering

Social engineering involves manipulating individuals into revealing information or performing actions that are beneficial to a criminal. A short film demonstrated how easily personal information can be obtained online through open source research (192.com for example) and data breaches. Skilled fraudsters can create a digital profile of their victim in as little as 90 seconds.

Oversharing online and using incorrect privacy settings can significantly increase the risk of fraud.

CIFAS (Fraud Prevention Charity) recommends:

- Never share sensitive personal details including you full name, date of birth, address and telephone number publicly. These are often used to answer security questions.
- Avoid posting upcoming holidays or photos revealing that you home is empty.
- Avoid posting photos of your children online in their school uniform.
- Do not click unknown links or accept requests from unfamiliar individuals.
- Keep profiles private and review your privacy settings regularly.

- Use unique passwords and do not share them via messaging services.
- Check your bank statement regularly and report any suspicious activity immediately.

Fraudsters often exploit emotions such as fear, guilt, urgency or trust. Common tactics include free offers and impersonation of loved ones or authorities.

Impersonation Fraud

Impersonation fraud involves criminals posing as trusted individuals or organisations to obtain money or personal information. Hackers frequently exploit commonly shared personal details or use software to guess weak passwords. Always verify unexpected messages, especially if they request money or sensitive information.

Artificial Intelligence

Gemma also discussed the risks posed by AI tools, including voice cloning and deepfakes (an artificially generated replicate image of a person). Eight out of ten parents have followers on social media that they have never met. This puts children in a particularly vulnerable position.

Criminals may use cloned voices in phone based scams known as **Vishing**. These scams can involve impersonating family members or using software to gain access to accounts using voice recognition. Gemma advised to hang up as soon as possible when scam calls are received to minimise the risk of your voice being spoofed for criminal activity.

Phishing and Spear Phishing

Phishing attempts via email, text (**Smishing**), or phone (**Vishing**) aim to trick individuals into revealing sensitive information. **Spear Phishing** uses personalised messages crafted through research or AI to increase the likelihood of a person becoming a victim.

Warning signs include poor grammar, unfamiliar senders, obscure email addresses, generic greetings and a sense of urgency.

Protective Measures

- Slow down and assess unexpected messages.
- Verify the sender directly using official contact information.
- Avoid clicking unfamiliar links or opening unexpected attachments.
- Limit personal details shared online.
- Use strong, unique passwords

Password Management

Common passwords (e.g. ‘password’, ‘qwerty’ or personal details) can be cracked within seconds. Using the same password across multiple accounts can increase the risk of compromise.

The National Cyber Security Centre (NCSC) recommends three random words plus three characters and checking whether emails or passwords have appeared in breaches via **HaveIBeenPwned.**

Password Managers are often built into your browser or device; however, they are also available as third party tools, and they can be used to securely store your passwords. Contrary to previous advice, writing passwords down and storing them securely away from devices is now considered an acceptable method.

Digital Hygiene

- Keep software and devices updated.
- Back up data to the cloud or to an external storage.
- Replace devices with unsupported operating systems.
- Regularly review privacy settings, clear browser cache and manage app permissions.

Public Discussion and Q&A

Gemma addressed concerns about "Whatsapp", confirming that although messages are encrypted, fraudsters can still attempt to send messages. Attendees also discussed mobile versus laptop security; banking apps continue to use a high standard of security, but those preferring laptops should ensure that they have up to date security software.

We asked whether a future practical session on topics such as cloud usage would be beneficial, and received positive feedback.

Scheme Update

- There are ongoing concerns with regard to speeding and pavement parking. These issues have been raised with our Community Policing Officer.
- Our new Neighbourhood Watch signage is now in place, and we are looking to order the laminate coverings for the older signs. A special thanks to our volunteers for assisting with putting them out.
- We thanked the 21 Young Hearts Café for their continued support of scheme.
- We raised the prospect of a specific email mailing list for attendees of our scheme.