Issue 19

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 2024

IF YOU DON'T DO ANYTHING ELSE, AT LEAST DO THIS!

Cyber Crime is a major concern with more people falling victim to this type of crime every day. But what are the quickest, most important things for you to do today to ensure it doesn't happen to you? There are 3 quick and easy steps you can take today to help to secure your accounts.

- Create a separate password for your email account(s)
- Use 3 random words
- Turn on two-factor authentication (2FA)

All your email accounts should have a unique and strong password. Since we all have so many passwords to remember these days, consider using a secure password manager. Email accounts are particularly important to protect, as once a hacker has access to your account, they are then able to access and change the passwords to all your other accounts including bank accounts.

Weak passwords can be hacked in seconds. Three random words is a recommended way of generating passwords, as it is easier to remember and takes many years for a computer algorithm to crack.

Start with your most important accounts (such as **email**, then **banking** and **social media**) and replace your old passwords with new ones. Do not use easily guessed words which can be found on, for example, your social media outlets. In addition to the words, use numbers, capitals and characters to add significantly to the number of combinations.

It has been said that 'two factor authentication' is time consuming and irritating, but it is in fact a really strong way to protect your data. Because, if you set this up, then even if the crook has your password, they still can't log in, by pretending to be you. Normal methods of authenticating might be a code or number sent to your mobile phone, which you have to enter onto your computer at log in. I find using your phones fingerprint or facial recognition is a very safe authentication method, since even if the thief has your phone, they will be unable to duplicate your unique fingerprint or face. It is also very quick and easy.

Check if the online services and apps you use offer 2FA – it's also called two-step verification or multi-factor authentication (MFA). If they do, turn it on. Start with the accounts you care most about, such as your email and social media. Banks, these days, tend to insist on 2FA, but check to make sure your bank has the correct mobile number for you.

Quarterly Tip

If it looks too good to be true.

It probably is!

CONTENTS

1 2FA / MFA
1 Quarterly Tip
2 Chair's Note
2 Corben's Corner
3 Unwanted Calls
3 Dodgy QR Codes
4 Key Safe?
4 Preserving Evidence

A NOTE FROM OUR CHAIR

Claire Wills

Since our last newsletter we have had our Annual General Meeting which we held this year at Boorley Green. Our aim is to move around so that everyone gets a chance to attend an AGM near their home. We are hoping to have the next one in the Hedge End area, so watch this space for more information next year! The AGM was well attended and we had 2 excellent talks from Local Bobby Simon Peacock and his boss Chief Inspector Matt Paling. We also had some local Parish Council Clerks attending and they, along with Eastleigh Town Council, have expressed an interest in promoting Neighbourhood Watch in their areas, so I will be working with them to facilitate this. A new(ish) coordinator, – Ben Britton, has expressed an interest in joining the committee and has attended our most recent meeting he has some excellent ideas and is willing to help in a variety of ways. Thank you Ben.

At a recent meeting with Eastleigh Police Inspector Andy Mooge the issue of Key Safes came up. I know that there have been reports of these being knocked off the wall so that the key can be retrieved and therefore access to the property gained. I asked Inspector Mooge how to avoid this and he had some very simple advice – put the key safe around a corner out of sight of the door! Apparently most key safes attacked have been next to the door and therefore have advertised that there is a key available! This makes sense – I know my family has put their key safes in a more discrete place, where someone who needs access to the key can find it, but not where it is visible from the doorway.

Keyless Entry Car thefts has again been highlighted in the news this week. We do have some Signal Blocking pouches that can be used to keep the car keys in to help prevent such thefts. Contact chair@eastleighnhw.org.uk to ask for them – they cost £1.75 each.

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

An issue I would like to mention in this edition is the use of Remote Access Tools (RAT's) and how scammers use them to scam people. I can clearly remember the first time I saw this working and it was with a company I was working for. I had a problem with my computer, so I raised a ticket to get it sorted. Well, shortly after I got an email from our IT dept requesting I do not touch my keyboard while the fix was applied. I duly sat back and watched, with a smile, as my mouse started to move around my screen and programmes were opened, changes made and my problem resolved. This is how a RAT works; it allows remote access to a person's computer which from a scammers point of view is gold. Now, these RAT's have to be downloaded onto the potential victim's computer and this is where the "persuasiveness" of the scammer is tested as they need to convince their intended victim to download the software onto their computer and further, then get the victim to allow the scammer remote access. This is normally achieved utilising scare tactics..... "*Your bank account is at risk however we (the scammers) can apply a patch to secure your money*", for example. This tactic is ALWAYS attached to a scam call and should prompt an immediate termination of this and any subsequent calls. Yes, the scammers may attempt several times to persuade their intended victim over several days to download a RAT, obviously all attempts must be resisted, however increasingly alarming their calls become.

ANYDESK is a download RAT commonly used by scammers although there are others. If a scam victim has been persuaded to download a RAT, the steps to take would be to seek specialist advice, as for as long as the RAT is installed on their device they are at risk, and it needs to be professionally removed and the device subject to a professional scan and clean to remove any further malware that may have been installed. Obviously, if access to any financial details have been compromised, then the Bank etc. must be contacted immediately for advice.

I know of a couple of computer repair shops who utilise RATs to support customer service operations. These, in my opinion, are perfectly legitimate.

Finally, I am aware of a certain band releasing tickets to concerts in 2025 and the disappointment felt when not being successful in securing tickets. All I can say to those disappointed people is .... don't look back in anger.

BEWARE OF DODGY QR CODES

QR codes are a great way to save time, enabling you to access websites without having to type in the address. However, QR links for payments can be tampered with by overlaying a rogue QR code, which directs you to a malicious site.

- Be careful what you scan – never just assume the QR code will take you where it says it will. If in doubt use another means of communication.
- If possible, go to the source: If you see a QR code you want to use, try instead to access the website directly by putting the address into your browser.
- If not, make sure that you know who has produced the code and someone has not tampered with or put their own sticker over the original QR code. When you scan, you should see the website address appear on your phone screen, so check it looks authentic before progressing further.

If you think you are the victim of fraud or scam, you should report this to Action Fraud (go to the Action Fraud website).

GETTING UNWANTED CALLS?

Modern phones have the advantage that you can usually see the number or the identity of the caller, which can help you decide whether to answer the call. However, as we have discussed before in Watch Word (WW18), numbers and identities can be 'spoofed', so you can't always trust what is shown on your screen.

Many more calls and texts, rather than being scams, are just nuisance calls. These are often from call centres, where the operator is trying to sell you goods or services. If you do pick up, you can often detect a call centre by the level of background noise. If you are getting these unwanted communications, there are ways you can strike back against them.

You can report the company to the Telephone Preference Service (TPS), your phone operator, Ofcom, Action Fraud, and the ICO.

If you're receiving unsolicited phone calls, you should contact the TPS. The TPS is free to use and is a register which records your preference not to receive unsolicited sales or marketing calls. If you've registered with the TPS and still receive unwanted calls, you can make a complaint to the TPS and it will investigate. Although the TPS is unable to prosecute, it does send complaints to the Information Commissioner's Office (ICO) which has the power to take action.

If you're still receiving harassing or unsolicited phone calls, you can talk to your phone company to report the phone number. Most providers offer products, services and advice - much of which is free - to block unwanted calls or reduce nuisance calls.

If you're registered with the TPS, third parties are not allowed to call you but some companies still do so. Third party marketing is when your details are sold on to numerous other companies for marketing purposes. Look out for tick boxes that request consent for your details to be passed onto third parties, if you do not want other companies to contact you, make sure you haven't ticked the box.

Texts can be reported by forwarding the message to 7726. This is the numeric digits for the word SPAM corresponding to the letters associated with the numbers on your phone's keypad. Your provider can investigate the origin of the text and arrange to block or ban the sender, if it's found to be malicious.

MAKE SURE YOUR KEY SAFE IS SAFE

There may be various reasons why you might choose to install an external key safe. If you live alone or you worry how help will reach you in an emergency, a key safe provides a convenient and secure way to store spare door keys. Maybe if you are going out for a run or to the gym, you may not want to carry a key with you. You may have children or relations who might require access to your house when you're out. If you have a self-locking door, you may be concerned about locking yourself out.

The obvious place to place the keysafe is next to the door where the lock is, but that is just where a potential burglar would look. It has been known for thieves to smash or prise the safe from the wall, so they can take it away to crack the code and access the keys.

- Make sure the key safe can't be seen from the road or by passers-by.
- Don't position key safes at eye level – this is where potential thieves will spot it easily!
- Don't put a key safe next to your front or back door where it's clearly visible.

- Install it correctly (or have a professional do it for you).
- Ideally, the key safe should be hidden out of sight but still receives some illumination for anyone that uses it.

KEEPING THE EVIDENCE

Forensic evidence

When a crime happens there may be forensic or fingerprint evidence we can gather. The person responsible for the crime may have touched surfaces, moved items, or left blood.

Preserving evidence and doing it quickly is important with forensics. Please tell us when you report your crime if you think there is forensic evidence. We'll let you know if the evidence is something we can use.

Steps you can take to preserve forensic evidence

- don't touch or clean any fluids such as blood
- don't touch or clean any areas or items handled by the person responsible for the crime

- if forensic evidence is outside, cover the area without disturbing any evidence. If you have to move anything, please try to handle it as little as possible and, if you can, wear gloves.
- if forensic evidence is on your clothing, please change out of these items and place them in a clean plastic bag.
- if there is any forensic evidence on your skin because the criminal grabbed you, tell us this as soon as possible and try not to touch or wash the area.
- If you need to clear up to make your home secure (eg broken window glass) please secure the window externally. Wear gloves and be careful not to touch the inside of the frame.

Digital forensics

Any CCTV system, doorbell camera, other video or audio recordings are valuable evidence. Don't switch off any devices or change any settings.

If possible, download footage to include 5 minutes before and after the incident and keep it safe. Don't delete it from the original device, as it is still evidence and may be needed later.

If you are unable to download the footage, leave the device on and record the time and date shown on the display. When you report the crime, explain you have digital evidence and we'll help you retrieve it.