

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 2022



SUMMERY ADVICE

By PCSO Victoria Amey

Now that we're beginning to see some warmer weather, and as many of us will be spending more and more time outdoors, as we enter the summer months, Hampshire Constabulary want to gently remind residents not to leave windows open or doors unlocked during this time.

Leaving the kitchen or living room window open, or even the back door, to allow for some fresh air into the house while you pop out for a short period of time might seem tempting, but this could provide an opportunity for someone to take advantage of the situation and commit a crime.

We want to offer up some friendly reminders around personal and household security at this time.

Most burglaries are committed by opportunists. A criminal may pick a house that looks unoccupied, has left a window or back-gate open or has little or no obvious security. These are often spur-of-the-moment decisions, made when they see valuables left on view or lapses in security. Car keys, left somewhere obvious can also be an attractive target.

By looking at your current level of security you can identify areas for improvement and reduce the risk of becoming the victim of burglary. Walk around your property – if you were locked out, where would you try to get in? Chances are that would also be where a burglar would try.



place. If you don't key lock the bolts in place they can be disengaged by simply pushing down the inside or outside handle. It's vital that

you remember to remove the key and to keep it away from the door out of sight. Remember to LIFT, LOCK and REMOVE.

Please do just take that little bit of extra care as we begin to spend more time outside the home.

As ever, we would ask the public to remain vigilant, and to report any crimes which are in progress or where there is a threat to life by calling 999.



Quarterly Tip

DEFINING Fraud and Scam

FRAUD - happens to you

SCAM - happens with you

You may also find that opportunistic burglars will knock at your door to see if you are at home. If they see you are in the back garden and have not heard the door they will try the front door. Many people are still lifting the door handle but not locking it while they are at home - this is not enough to secure the door and burglars often enter properties this way.

When you shut the door and lift the handle the hook bolts are thrown into the locking mechanism in the door frame. By turning the key the you are locking these hook bolts into

CONTENTS

- 1 *Window warning*
- 1 Quarterly Tip
- 2 *Chairman's Note*
- 2 Corben's Corner
- 3 *Bank Notes*
- 3 Stamping Out
- 3 *Car Thieves*
- 4 Scam Revenge
- 4 *WIDE(N)*
- 4 Flip Flops

A Note From Our Chairman

Mike Anthony



I'd like to share with you about something we learned at a recent meeting with the Hants Pol Cyber Crime Unit and fellow Cyber Champions held to discuss requests for help and latest cyber threats. One topic discussed was that of social-media related crimes and we heard that a significant

proportion of the Unit's time is currently taken up by these forms of crime. They typically include ransom demands, sextortion or compromised social media accounts being used by criminals to provide contact information or hide their activities. This obviously tends to be the younger members of society (but not always) and the effects of the crimes on the young victims should not be underestimated - we have seen in the media that, in the worst cases, the victims can be driven to consider suicide.

For example, a young person (often male) may send compromising photos of themselves to someone they have, or believe they have, a close relationship with. Later the relationship may break down and the photos then used to blackmail, distress or pressure them. This is sometimes referred to as 'revenge porn' or 'image-based abuse'. Sometimes the relationship has only been online and the victim is horrified to find that the person to whom they have been sending personal info and photos is not the person they believed them to be - when they receive extortion demands.

So, if you have young children, or grandchildren, active online and maybe at college or starting



Lots more information can be found on our ENWA website

www.eastleighnhw.org.uk/

and also take a look at our [Facebook](#) page



university, it is worth having a conversation with them about recognising the privacy of their, or other people's, images or other private information, that abuse could be an offence and the importance of using strong passwords and 2 Factor Authentication to protect their social media accounts.

It could save someone a lot of distress.

Corben's Corner

By John Corben

Scammers are always adapting and thinking up new ways to con people, Covid related scams, Valentine's Day scams, parcel delivery scams and so on.

I want to talk firstly about **Phone Number Spoofing**. This is changing the incoming number the victim sees on their phone to one such as 0800 318 665, which is the phone number of Barclaycard fraud reporting line. The potential victim would be asked by the fraudster to check this number, and it would check out, adding authenticity to the fraud attempt. Once this 'trust' has been established the scam could proceed. There are **NO** circumstances where any major Bank or financial company would approach a member of the public in this way, so should cause alarm bells to ring. A way to confirm this is a scam is to hang up and call the relevant Bank etc from a separate phone and discuss the call with them.

Secondly I would like to warn everyone about **Remote Access Control**. This is a programme



downloaded onto a computer, phone or other electronic equipment which allows a third party to remotely access and control all the functions on the victim's device. Typically a scammer, having convinced a person that

their money or other valuable documentation is at risk, persuades the victim to download a programme, so they can help them. However far from helping the victim, this programme, once downloaded, can allow the scammer to control the victims device with usually disastrous financial results. Never be persuaded to download any programme which would allow remote access to any device following an unexpected third party contact.

Finally I would like to remind everyone that **FREE** help can be sought to answer virtually any scam attempt questions from our Cyber Champions. They can be contacted at hampshirecyberwatch.org

TIME RUNNING OUT FOR LARGE DENOMINATION NOTES

If you have a big stash of £50 or £20 notes under your mattress then you only have a short time to spend them. The original paper notes were replaced in 2020 for the £20 and 2021 for the £50, by new polymer notes. These have the benefit of being much more durable and have many more security features to reduce the risk of forgeries.



pay the bearer on demand the sum of x pounds’.



Both the old and the new notes feature the

same picture of the Queen, from a portrait painted when she was 59. However, they do have different famous individuals on the back. The economist Adam Smith has been replaced by the painter JMW Turner on the twenty. The paper fifty had two people, entrepreneur Matthew Boulton and Engineer James Watt who have been superseded by the Enigma Code breaker Alan Turing.

The Bank of England have worked with GCHQ to design a series of puzzles, based on the Turing £50 note design. You can test your code breaking skills where you will have to solve 11 puzzles, each based on one of the features on the note. Solve all 11, and you will have all the clues you need to solve the final puzzle. <https://www.gchq.gov.uk/information/turing-challenge>

AND STAMPS

If you have old Christmas stamps you CAN continue to use them after 31 January 2023 following a Royal Mail U-turn. The postal service had initially announced, as part of a wider shake-up, that Christmas stamps would be replaced by new barcoded versions from 31 January 2023. This would have rendered old festive stamps useless unless swapped.

But while Royal Mail says it will still add a barcode to new Christmas stamps, it's confirmed that "following discussions with key stakeholders, including feedback from our customers", non-barcoded Christmas stamps will remain valid.

The U-turn means you can continue to use Christmas and "special" commemorative stamps, such as the *Doctor*



Who collection, after 31 January 2023 – and they don't need to be swapped for barcoded alternatives.

Any other stamps, however, including all those with the Queen's head on them that say '1st' or '2nd' class, or any other price, will not be valid after 31 January 2023. You will need to swap them for a barcoded version (see below for more on this) or pay an as-yet-undisclosed surcharge to continue to use them.



BEWARE OF OPPORTUNIST CAR THIEVES



Following some opportunist vehicle content thefts locally, the Police issued the following advice:

- When leaving your vehicle, close all windows and **lock your car**.
- Upon locking your vehicle test the door to ensure it is actually locked.
- Park your vehicle in an attended car park.
- Look for public car parks approved by the Park Mark scheme.
- When parking at home, use your garage. If you don't have a garage, park in a well-lit area if possible.
- Don't leave anything on display in your vehicle.
- Take all your personal possessions with you.
- Do not hide any valuable items. Take it with you or leave it at home.
- Leave the glove box open to show there's nothing inside.
- Do not store ownership documents inside the vehicle.

FIGHT BACK AT THE SCAMMERS

Have you received an email that you are pretty certain is a scam? Obviously you need to delete it, but before you do, you can potentially get your own back on the scammers by forwarding the email to the National Cyber Security Centre.

They analyse the contents, and if they conclude that the email is malicious, they can block the scammer's email address, and work with website hosts to remove links to rogue sites. They work together with government departments and law enforcement partners to deal with potential crimes.

The address to forward your suspicious emails to is: report@phishing.gov.uk. They will send a standardised reply to you which contains links to useful security information.

How to recognise a scam message: Scammer's will often disguise their email address so it appears official. If you hover your cursor over the sender's address it will show the real address, often a 'gmail'. If there is a click link, **don't click** but hover your cursor over it and the destination should appear in the bottom left corner. It should be obviously bogus. The text may be telling you that you must act quickly or offer incentives to reply. If you're worried that it might be genuine, **don't** reply to it or use links or phone numbers from the email, but check contact details from their official website.



National Cyber
Security Centre

WORRIED ABOUT BURGLARY? THINK WIDE(N)



-  **WINDOWS** LOCKED
-  **INTERIOR** LIGHTS ON A TIMER
-  **DOORS** DOUBLE OR DEADLOCKED
-  **EXTERIOR** LIGHTS ON A SENSOR
-  **(NEIGHBOURS)** KEEP AN EYE OUT



TO FLIP FLOP OR NOT?



With the summer upon us, there is some debate about whether driving in flip flops or barefoot is illegal. It seems that Highway Code text is advisory rather than

mandatory, stating that footwear "does not prevent you from using the controls in the correct manner." If you were to be involved in an accident, and footwear can be seen as contributing to the outcome, then you may be liable for a "driving without due care and attention" charge, with the risk of fines and points on the licence.