Ferring

NEIGHBOURHOOD WATCH

Quarterly Edition October 2019

Correspondence to : Ferring Neighbourhood Watch
c/o Ferring Parish Council, 1 Elm Park
Ferring, BN12 5RN
Email: FerringNW@ hotmail.com Tel: 01903 249449

Action Fraud have received an increase in reports and intelligence where elderly victims are being targeted by individuals claiming to be police officers or traffic wardens. The victims are being approached whilst parked in a car park and are told by the suspect that they have parked illegally or broken a speed limit and a photo has been taken of their car for 'evidence'.

Victims are advised that they will face a substantial penalty fine unless they pay a smaller upfront fee immediately. Victims, who opt for paying the smaller penalty, will be directed to a parking meter and asked to enter their card and PIN. These parking meters have been tampered with by the suspect in order to retain the card.

Once the victim inserts their card and are prompted for their PIN, the victims are watched closely over their shoulder by the suspect, for their PIN. Once victims input their PIN, the card is retained by the machine, and victims are told by the suspect to seek help from the company who operates the parking meter or their bank.

What you need to do:

- If you are suspicious about the authenticity of the fine, do not pay it until you have verified it with your local council.
- Always shield your PIN from view when using an ATM machine, and never share your PIN with anyone.
- If your bank card is retained by an ATM machine, contact your bank immediately to inform them.


Keep your vehicle safe and sound

Top Tips

Safer ARUN PARTNERSHIP

1. **Lock it!** Make sure your car is always locked whenever leaving your vehicle unattended. You may not be insured if the car is left unlocked!
2. **Close the windows and sunroof** Don't give thieves the opportunity to go 'fishing' for your things by reaching in through open windows by hand, or using items like bent coat hangers to open doors.
3. **Remove your keys** Never leave the keys in the ignition, even if you're just stopping for a newspaper, paying for fuel, or defrosting your windscreen on the driveway. Again, you will probably not be insured!
4. **Take it with you** Opportunist thieves find your mobile phone, change for the car park, sunglasses, watches, coats, bags, and even medication, irresistible, even if you think they are of no value. It goes without saying that wallets, handbags, purses and credit cards should never be left in unattended vehicles.
5. **Lose your Sat-Nav** Remove your sat-nav and its holder, and wipe away any suction marks as these could alert a potential thief to the possibility of a sat-nav, smartphone or other device being stored inside the vehicle.
6. **Remove your documents** Never leave vehicle documents in your car; don't make it easy for a thief to sell your car or provide a believable cover story if stopped by the Police.
7. **Keep keys safe at home** Be aware of your keys and store them safely. Don't leave them lying around or visible in pockets. Don't leave them visible on a window sill in your home or near the front door where they could be 'hooked' out through the letterbox. If you have a keyless system, make sure you keep the key out of communication range; if you don't, your vehicle will remain unlocked.
8. **Secure things on the outside** Things left on roof and tailgate racks, in roof-top boxes or tool chests can easily be stolen when your vehicle is parked. Secure these things by using padlocks or cable locks and secure them to the vehicle, but always try to avoid leaving belongings in them if you can.
9. **Park Safely** Whenever you can, park in well-lit and busy areas where the chances of a thief being caught increase, so they will probably steer clear.

www.arun.gov.uk/safer-arun-partnership

The 'Safer Arun' Partnership are promoting the message that the majority of car break-ins in the district are to vehicles that have not been locked (*'insecure'* in police jargon).

The title for social media posts on this topic is "***LOCK IT! To avoid opportunistic thieves taking things from your vehicle, make sure it is locked. If left unlocked, it is unlikely your insurance will be valid***."

This seems obvious, but many people are being caught out. Please take note.

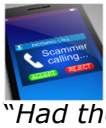
A 'Top Tips' card has been produced (*left*), which can be obtained free of charge – please contact me using the details in the Correspondence section at the top of this newsletter, if you would like a copy.

TOKYO 2020 qatar 2022

Beware! A scam 'International Postcode Online Lottery' letter is turning up in people's post. It appears to have been given a refresh as fraudsters attempt to catch more people out. Previous versions of this letter mentioned the 2018 football World Cup, which has now been updated to Qatar 2022.

continued overleaf …

(continued from overleaf) Similar 'Fifa lottery' letters have recently been the subject of warnings by Action Fraud and Trading Standards. The probable aim is to dupe someone into giving away their bank details, or to get them to make a cash payment in order to 'release' fictional winnings.



Another scam warning: Fake phone calls from the 'Visa' fraud department. Which? have received reports in recent weeks of a complex 'Visa' scam doing the rounds again. The reports of these 'newer' version of this scam appear to vary – here is an example:

"*Had the same phone call on my landline this morning saying £300 spent in Tesco's and £650 at Harrods. The guy was very convincing saying not to divulge any information to him but said within an hour I would receive a phone call from the Bank's fraud section. Shortly after I received an international incoming call which I ignored. In the meantime I contacted my bank and it confirmed that no transactions had been made. Hope these responses help to inform others of this scam*."

Advice from Surrey & Sussex Police Economic Crime Unit …

Help secure your online accounts with these strong password tips. Using a strong password is a vital part of your online security. Often online security is breached because a password has not been changed for years, or used multiple times for different accounts.

There are a number of ways to make your passwords more secure and protect yourself from a potential hack:

- Make a password as long as possible.
- The more characters it has, the harder it is to crack - aim for a minimum of 13 characters.
- Use different types of characters, including numbers, symbols and punctuation marks
- Don't include only dictionary words in your password as this makes them easier to crack
- Avoid personal names, like family, pets, or sports teams.
- Use different passwords for different accounts, especially for your personal email account. This way, if one password is compromised then at least only one account can be hacked.

Check to see if you have an account that has been previously compromised in a data breach by entering your email address on this email checker tool website: *https://haveibeenpwned.com*

You may want to review your password security as a result!

Banks and retailers are set to introduce stringent new security checks, with customers asked for additional verification when shopping online, logging onto their account or making contactless payments. The EU 'Payment Services Directive' (PSD2) is intended to enhance payment security and reduce fraud, and payment providers within the EU are now legally required to check that it's really you making the purchase – known as **'strong customer authentication' (SCA).**

Instead of asking only for your name and card details when you shop online, retailers and banks should be making extra checks, such as asking for a one time passcode (OTP) sent via simple text to your mobile. This should reduce 'card not present' fraud, which cost the UK £506m last year.

What is strong customer authentication (SCA)?

The new regime of 'strong customer authentication' or SCA means that banks must identify every customer using at least two of these independent factors:

- Something only you know (a password or PIN code)
- Something only you possess (a card reader or registered mobile device)
- Something that identifies you uniqely - a digital fingerprint or voice pattern.

If this isn't possible, payments will be declined, although certain low-risk payments will be exempt.

Mobile and Internet provider EE has been fined £100,000 by the Information Commissioner's Office (ICO) for sending 2.5 million illegal marketing texts without having consent to do so. The messages encouraged customers to access and use the 'My EE' app to manage their account and upgrade their phone. Marketing messages can only be sent to existing customers if they have given their consent and if they are given a simple way to opt out of marketing.

NHW locally is pursuing the Sussex Police & Crime Commissioner (PCC), Katie Bourne, about overdue response improvements with the 101 crime reporting telephone line. The PCC has acknowledged publicly that the 101 service is not good enough and has said she is taking an interest in the matter. A response from her on that matter is awaited.

Older people targeted by criminals in mail-based scams are being 'groomed' by perpetrators, say Neighbourhood Watch who are calling for accurate language to be used when talking about this type of fraud. The NHW Network says the process older people are subjected to, when being scammed out of their savings, has similarities to the insidious and manipulative techniques practiced by child grooming gangs. The effects of fraud upon older people can be devastating - a victim of doorstep crime is 2.5 times more likely to either die or end up in care within two years compared to their 'non-scammed' neighbours, according to research from the Association of Chief Trading Standards Officers.