Brindle Parish Council: local information

Welcome to May's Parish Council alerts. This month, we have advice on protection – for both your car and for your email and social media accounts. There's also, as usual, a range of scams to avoid.

PROTECTING YOUR CAR

One car is stolen every ten minutes. Most car crimes happen because cars are left unlocked. There is a misconception that some cars are auto-locking and lock themselves if left unattended after a period of time. This isn't always correct. Another misconception is that your car is too old and no one will bother stealing it. This is also incorrect – both new and old cars are at risk. The good news is that there are simple steps everyone can take to help reduce the risk to their car.

The Neighbourhood Watch charity suggests that, to protect your car, keep it locked, lit and empty. 44% of cars are broken into via an unlocked door. 80% of car crime occurs during the evening or at night and parking near street lamps or in a busy area can deter thieves. Also, owners often forget that personal belongings within the car are at as much risk of being stolen as the car itself.

PROTECTING YOUR ONLINE ACCOUNTS

If a hacker got into your email or social media account, what would they find? Health and banking information? Names and contact details for your friends and family? Private photos and messages? For most people, it's at least one of these. Between February 2020 and February 2021, Action Fraud received 15,214 reports about email and social media account hacking. The majority of reports (88%) were made by individuals not businesses. Facebook, Instagram and Snapchat were the most affected social media accounts, with phishing messages being the most common tactic used by cyber criminals to lure unsuspecting victims. Some victims are extorted for money, whilst others have their accounts used to send malicious links to their contacts. One victim who had multiple email and social media accounts hacked paid over £2,000 to regain access to them. Another victim reported that her hacked Facebook account was used to trick her friends into sending money into a PayPal account they thought belonged to her.

Secure your email and social media accounts by:
1: Using a strong and separate password for your email, as well as for other accounts such as your banking or social media accounts.
2: Enable two-factor authentication (2FA). It will help to stop hackers from getting into your online accounts, even if they have your password.
3: If you can't access your account, search the company's online support or help pages. You'll find information about how to recover your account.

For detailed instructions on how to reset your password or enable 2FA on your accounts, visit: https://www.actionfraud.police.uk/secureyouraccounts.

SCAMS

HMCTS SPOOFING PHONE CALL

Beware receiving a call alleging to be from the HM Courts and Tribunals Service (HMCTS). Scammers mimic legitimate phone numbers (spoofing) and may allege that you owe HM Revenue and Customs (HMRC) money and that a warrant for your arrest has been issued. Scammers may also tell you to look up contact details for HMCTS to verify the number they are using to call. Note that HMCTS is separate from HMRC and will not call or email you about tax matters. If you

receive a call or email, or any type of contact, do not provide any personal details or make a payment.

SCAM WARRANTY TELESALES
Use caution if you are contacted by a telesales call offering to sell you a warranty or home appliance insurance. While many cold calls are trying to sell a new policy, many claim your existing cover is expiring and you need to renew, regardless of whether you had cover in the first place. Householders suffering from dementia have been particularly targeted, with attempts to sell insurance for items that the householder does not own or worth considerably less than the cost of the insurance. Businesses offering insurance policies should be registered with the Financial Conduct Authority who also offer an ombudsman scheme. Check the register at www.fca.org.uk.

PHISHING SCAMS
Be on the alert for a phishing email purporting to be from TV licencing that states that due to outdated TV account details, your account will be suspended unless you provide your date of birth, current address, telephone number and payment method. The email provides a link to 'Visit TV licencing now'.

Beware of a fake *Sainsbury's* email stating you have been selected to participate in a gift card giveaway. The recipient is invited to enter personal information on a linked website. Similarly, be on the alert for a phishing email alleging to be from *Just Eat* offering a £50 gift card, again taking you to a link requesting personal details. Also doing the rounds is a phishing email alleging to be from *Yahoo* asking you to upgrade 'here'. There is a *DVLA* phishing email from the email address: 'G.O.V.U.K'. This states that payment for your latest vehicle tax invoice failed and that some of the billing details associated with your account might have expired or were otherwise changed. You are invited to click on a link to a secure page to enter your details.

Phishing emails can look as if they have come from a trustworthy entity and can make you panic into divulging personal information, often implying a service will be withdrawn or you will not be 'legal', or tempt you by the lure of a refund or a voucher. If you have received a suspicious email, forward it to the Suspicious Email Reporting Service (SERS) at report@phishing.gov.uk. Scams can also be reported to Action Fraud. Contact them on 0300 123 2040 or at www.actionfraud.police.uk.

Keep safe and well!

Brindle Parish Council