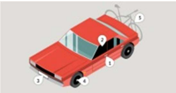
Ferring

NEIGHBOURHOOD WATCH

Quarterly Edition July 2019

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



HAVING YOUR CAR BROKEN INTO AND LOSING YOUR POSSESSIONS to thieves can be very distressing. Here are a few simple actions you can take to keep your vehicle, and what's in it, safe.

- **ALWAYS lock your car** - we all know how easy it is to turn your back for a moment and forget your vehicle is unsecured. Get in the habit of locking your vehicle, even if you're only going to be away for a moment.
- **Close windows and the sun roof to prevent 'fishing'** - leaving windows and the sunroof open invites fishing for items through the gap by hand or with, say, a bent coat hanger, which could also be used to unlock a door for them to get in. Thieves can be ingenious, don't give them the opportunity.
- **Secure your number plates with tamper-resistant screws** - the easiest way to change the identity of a stolen vehicle or avoid speeding tickets and parking tickets is to fit stolen number plates. Using security screws (*e.g.* from Amazon) to attach your vehicle's number plates makes it harder for thieves to get your number.
- **Take it with you or hide it** – your mobile phone, coins for the car park, sunglasses, packs of medication or other items that can earn quick cash are irresistible to the opportunist thief. Remember, the cost of replacing a smashed window is often more than that of what's stolen. Wallets, handbags, purses and credit cards should never be left in an unattended vehicle, not even in the boot; you may have been observed putting them there.
- **Hide electrical items and leave no clues** - leaving sat nav mounts, suction cup marks on windows, or cables on view gives it away that you may have left a sat nav, smartphone or other valuable device in your car. Even if they can't see the device, they might still break in to see if it's stored in the car, out of sight.
- **Never leave vehicle documents in the vehicle** - having registration and insurance documents could let a thief pretend to be the owner, which means they could sell it on quite easily. Not what you want.
- **Park in well-lit and busier areas** - it can take less than 30 seconds to break into a vehicle. Parking in well-lit areas and busy streets increases the chances of a thief being seen, so they'll probably look elsewhere.
- **Choose your car park wisely** - always try to park in well-lit and staffed car parks or those with a Park Mark safer parking award. To find one, simply check out Park Mark (*http://www.parkmark.co.uk/car-park-finder*).

COURIER FRAUD, BOGUS POLICE AND BANK OFFICIALS ALERT. Individuals have been receiving phone calls from people claiming to be a police officer or banking official.

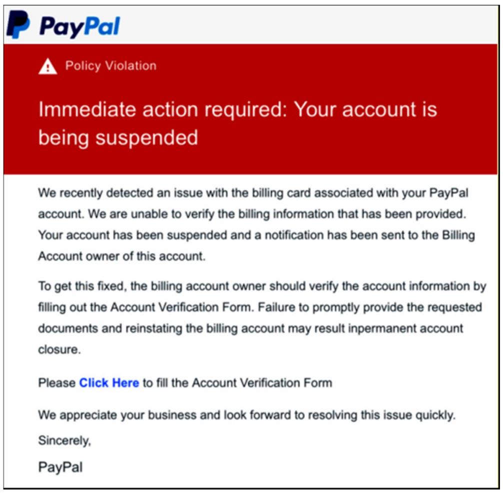
The caller will say either:

- There has been fraudulent activity at the victims' bank and the staff at the bank are involved, the victim is then asked to withdraw money to either keep it safe or assist the police with their investigation …
- A business such as a jeweller's or a currency exchange has committed fraud, and they require the victim's assistance to help secure evidence. This may be by purchasing jewellery, or exchanging an amount of currency to hand over to the police …
- The victim's card has been compromised and used to purchase goods by a suspect. The victim is requested to withdraw their money to keep it safe or hand over their bank card to the police.

Remember - YOUR BANK OR THE POLICE WILL NEVER:

- Phone and ask you for your PIN or full banking password …
- Ask you to withdraw money to hand over to them for safe-keeping …
- Ask you to transfer money out of your account …
- Send someone to your home to collect cash, PINs, cards to cheque books.

BEWARE FAKE EMAILS FROM PAYPAL - The email shown below was received by a Neighbour Watch member. Is it fraudulent or not? What would you think?



PayPal

Policy Violation

Immediate action required: Your account is being suspended

We recently detected an issue with the billing card associated with your PayPal account. We are unable to verify the billing information that has been provided. Your account has been suspended and a notification has been sent to the Billing Account owner of this account.

To get this fixed, the billing account owner should verify the account information by filling out the Account Verification Form. Failure to promptly provide the requested documents and reinstating the billing account may result inpermanent account closure.

Please Click Here to fill the Account Verification Form

We appreciate your business and look forward to resolving this issue quickly.

Sincerely,

PayPal

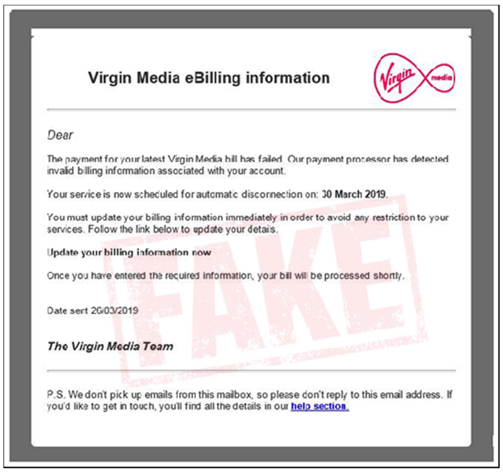
PayPal say they will:

- **ALWAYS** start emails with your first and last name or business name.
- **NEVER** ask for bank or security information.
- **NEVER** ask for your full name, password, or answers to your PayPal security questions in an email.
- **NEVER** ask you, as a seller, to provide tracking numbers for dispatched items before you've received payment into your PayPal account.

Further professional advice is:

- **ALWAYS** be suspicious. Is the email unsolicited? If so, be sceptical.
- **NEVER** click on any links or requests for information.
- **HOVER OVER** the **sender email address** in the header: Does it EXACTLY MATCH the company name? In the example email shown, the sender was *test@racscleaningmalta.com*, not PayPal. That's an immediate give-away.

FRAUDSTERS SEND FAKE VIRGIN MEDIA EMAILS



Virgin Media eBilling information

Dear

The payment for your latest Virgin Media bill has failed. Our payment processor has detected invalid billing information associated with your account.

Your service is now scheduled for automatic disconnection on: **30 March 2019**.

You must update your billing information immediately in order to avoid any restriction to your services. Follow the link below to update your details.

Update your billing information now

Once you have entered the required information, your bill will be processed shortly.

Date sent 26/03/2019

The Virgin Media Team

P.S. We don't pick up emails from this mailbox, so please don't reply to this email address. If you'd like to get in touch, you'll find all the details in our help section.

Action Fraud has received over 100 reports about fake emails that purport to be from Virgin Media. The emails threaten the recipient with "automatic disconnection" due to "invalid billing information".

Of course, if you're not a Virgin Media customer, you can ignore it completely.

The links in the emails lead to genuine-looking phishing websites that are designed to steal your Virgin Media account login details.

DON'T CLICK on the links or attachments in suspicious emails, and never respond to messages that ask for your personal or financial details.

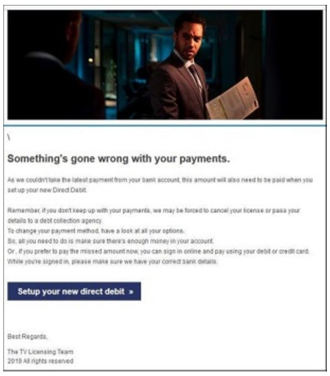
For more information on how to stay secure online, visit www.cyberaware.gov.uk.

PREGNANCY AND PARENTING CLUB FINED £400,000 FOR SHARING PERSONAL DATA UNLAWFULLY.

The Information Commissioner's Office (ICO) have fined Bounty (UK) Limited £400,000 for illegally sharing the personal information of over 14 million people with marketing agencies and other companies.

The information was collected directly from new mothers and in some cases at hospital bedsides. Bounty collected this information for membership registration, but it also included the date of birth and sex of the child, and went on to share that personal data – that is illegal.

BEWARE OF TV LICENCING EMAIL SCAM, "YOUR DIRECT DEBIT HAS BEEN CANCELLED"



Something's gone wrong with your payments.

As we couldn't take the latest payment from your bank account, this amount will also need to be paid when you set up your new Direct Debit.

Remember, if you don't keep up with your payments, we may be forced to cancel your license or pass your details to a debt collection agency.
To change your payment method, have a look at all your options.
So, all you need to do is make sure there's enough money in your account.
Or, if you prefer to pay the missed amount now, you can sign in online and pay using your debit or credit card.
While you're signed in, please make sure we have your correct bank details.

Setup your new direct debit »

Best Regards,

The TV Licensing Team
2019 All rights reserved

This is quite the most convincing email scam that I have personally come across, so much so that when I received it I felt it necessary to go into my bank account to check that there was nothing amiss with my monthly TV licence direct debit payments. All was OK, as I hoped and expected.

The thing to realise about this is that this scam is clever in many ways: it uses a still from the recent advert about TV licencing, it is written with good English without any grammatical or spelling mistakes, and it is short and to the point. I fear that many people would succumb to this inducement, if they weren't sufficiently sceptical of its origin.

There are two give-aways though, apart from making untrue claims. The first is glaringly obvious, the sending address; "root @ pepsistore.com", clearly suspect. That is always what I first check when I'm suspicious of an email I'm not expecting. Another give-away is the URL embedded in the "Set up your new direct debit" hyperlink (right-click on the button to see that); I won't repeat it here, but again it is suspect. Maybe these criminals are not so clever after all. **Watch out for this scam landing in your Inbox, and don't be taken in by it.**

TALKTALK'S FREE CALL-SCREENING SERVICE – CALLSAFE – WORTH CONSIDERING.

TalkTalk are offering users of their landline phone package a useful service included for no extra charge - they call it 'CallSafe'. It is a telephone call screening service, that can be configured to reject calls by cold-callers, by virtue of their calling numbers being unknown to you. If you're already a TalkTalk customer, and if you don't already use a different call-screening service, this could be very useful to you. I have used a different call-screening service myself for a couple of years, and I haven't received a single nuisance call in that time, having been pestered by them regularly before that.