Dear Residents **October 2016 – bulletin 10**

**Crime reports**

Police report that petty crimes this month include sheds broken into all around our area along with theft and damage to some vehicles. Their main message is to prepare your home, car and bicycle for the darker autumn/winter evenings including checking lights, tyres and wearing light clothing when cycling. Also, leave lights on at home when out, preferably controlled by timers to come on randomly or by sensors to detect movement outside. They recommend that cycle frame numbers are registered on [*www.immobilise.com*](http://www.immobilise.com)(you need make, model, code and photos). [*www.soldsecure.com*](http://www.soldsecure.com) can identify a decent D-lock for you. Consider buying a cycle anchor to bolt to the wall or floor and beware of being too specific about your home address if posting “track My Ride” results on social media.

Police continue to warn of bogus cold-callers intent on taking advantage of us by saying they are from the local authority, health services, utility services or simply are trades people looking for business (fixing roofs, mending drives, selling products). “Nottigham Knockers” claim to be reformed criminals trying to make a new life or claim to be disabled and need to pay for a carer (the scam originated in Nottingham but now nationwide). They offer a range of cleaning products but really are sizing up your property for a burglary some weeks later.

**More scams**

(a) One resident emailed me this month about a caller purporting to be from nPower and asking for meter readings and account number. Quite rightly, he refused to respond and nPower failed to validate it when enquiring with them later - if in doubt, play safe.

(b) Someone must have acquired the email addresses of BT customers (possibly due to the Yahoo hacking publicised in the media recently) as I continue to receive requests to use links to “update your BT billing details” or to “revalidate your account”. I reported these to [*www.NFIBPhishing@city-of-london.pnn.police.uk*](http://www.NFIBPhishing@city-of-london.pnn.police.uk) who have an automated process and are keen to receive as much info as possible to tackle them and send out warnings. They are the source of the warnings from the national Neighbourhood Watch network.

(c) One clue about these scam emails is how they are vague in addressing the “customer”. My experience includes “Dear User”, “Dear Valued Customer” or even “Dear Sir/Madam”. The latest was pretending to be from Barclaycard addressed to “Dear Important Customer – Your new tax payment is now Overdue”. I suppose someone must fall for it but hard to believe when they look so juvenile.

**Warning from national Neighbourhood Watch – security of WiFi hotspots**

* Try not to use insecure public Wi-Fi hotspots (e.g. cafes, pubs, hotel rooms, airports) if doing anything confidential, such as logging on to accounts. Use commercial hotspot providers like BT OpenZone or T-Mobile as these are known to be secure.
* Just being given an access code or asked for an email address doesn’t mean security.
* Alternatively, use a mobile broadband dongle set to secure – slower but safer.

Some criminals are known to set up fake hotspots on their own laptops. Also, real hotspots in cafes, airports, etc. can be hijacked.

Robert Mills