Dear Residents  **May 2017 – bulletin 4**

**Crime reports**

* Cars/properties damaged and two secure properties in Pocklington broken into and searched.
* Sheds at Market Weighton allotments damaged or broken into and tools/equipment stolen.

**Scam reports – local**

These evil people will try anything – how about this recent report of a tempting offer (oops – from a French email address):

* “You have an outstanding **tax refund of £565.84 GBP** for the tax year……follow the instructions………payments processed within 3 to 5 days…….HM Revenue & Customs.”

**Reports from the national Neighbourhood Watch team**

* Several cases of **a lone fraudster purporting to be unfamiliar with the local area**……..make an excuse to talk to victim (e.g. directions or recommend good local hotel)……..several others intervene and pretend to be plain clothes police (inc. false identification)……..then ask to examine fraudster and victim’s wallet/purse……..later find contents or possessions missing.
* Very recent and ongoing **Ransomware cyber attack on businesses** – Friday 12 May saw widespread disruption due to cyber criminals locking files remotely……….devices can be infected through links in unsolicited emails or through a security vulnerability in the software you use. Protect yourselves by:

1. Install system and app updates as soon as available;
2. Install anti-virus software on all devices and keep updated;
3. Create regular backups to a device not left connected to your network.

Go to <https://www.ncsc.gov.uk/guidance/ransomware-latest-ncsc-guidance> for the National Cyber Security Centre technical guidance including software patches that will prevent “Wannacry” infection. Additional help at <https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware>.

For **Ransomware protection for individuals,** follow (a) to (c) above and only install apps from official stores (e.g. Google Play Store; Apple’s App Store) as they offer better protection than 3rd party stores. Jailbreaking, rooting or disabling default security features will make your device more susceptible.

**Warning from the national team**

* Fraudsters may exploit this Ransomware incident to use in **phishing/smishing campaigns**……..be cautious if receiving NHS emails as they can be spoofed……..do not open attachments or click on links if the email is unsolicited.

Robert Mills