Dear Residents  **April 2017 – bulletin 3**

**Crime reports**

* Parked cars in Pocklington and Market Weighton damaged. Also, sheds/buildings accessed but not in our villages.

**Scam reports – local**

Unsolicited emails continue to be reported which all want us to reply back via a link. The main themes are:

* “We’ve removed a virus from your email…………click below for the original message………”
* [From “Adobe Acrobat Pro DC………………..you have received a document: Overdue Invoices.pdf………....view document here.”](mailto:From%20mark.acctspay@itsol.co.uk)
* From “Barclays………………there was an attempt to sign in to your Barclays online from an unrecognized device…………..….you are hereby requested to perform some necessary information update.”
* From “Argos………we encountered a problem with your account…………..click here to verify account status………….……we apologise for any inconveniences caused.”

In addition, reported unsolicited telephone calls appear to be increasing from foreign-sounding people wanting to tell us we have internet or computer problems and want to help us resolve them.

***CLEARLY SOMEONE IS FALLING FOR THESE DESPICABLE SCAMS OR THEY WOULDN’T BOTHER TRYING IT ON – FINANCIAL FRAUD COSTS THE UK £2 MILLION PER DAY.***

**Scam report – national**

A high volume of phishing emails to personal and business addresses pretending to come from various addresses. Subject line has recipient’s name – main body of text goes:

*“Hi, [name]. I am disturbing you for a very serious reason. Although we are not familiar, but I have significant amount of individual info concerning you. The thing is that, most likely mistakenly, the data of your account has been emailed to me. For instance, your address is [real home address]. I am a law-abiding citizen, so I decided to personal data may have been hacked. I attached the file – [surname].dot that I received, that you could explore what info has become obtainable for scammers. File password is – 2811. Best Wishes.”*

The attachment is thought to contain the Banking Trojan Ursniff/Gozi hidden within an image. Having up-to-date virus protection is essential but will not always prevent infection of your device.

* **Do not click on links or open attachments** – they can spoof addresses so they appear to be from a trusted source.
* **Do not enable macros in downloads** as this will allow malware installation.
* **Install software updates** as soon as available.
* **Back-up important files** to an external hard drive, memory stick or online storage.
* **Contact your bank** immediately if you suspect your details are compromised.

Robert Mills