Pittsfield Charter Township
Department of Public Safety

6227 West Michigan Avenue, Ann Arbor, MI 48108
Phone: (734) 822-4911 • Fax: (734) 944-0744
Website: www.pittsfield-mi.gov

Matthew E. Harshberger
Director of Public Safety
harshbergerm@pittsfield-mi.gov
(734) 822-4921

Mandy Grewal, Supervisor

Bi-Weekly Public Safety Activity Summary
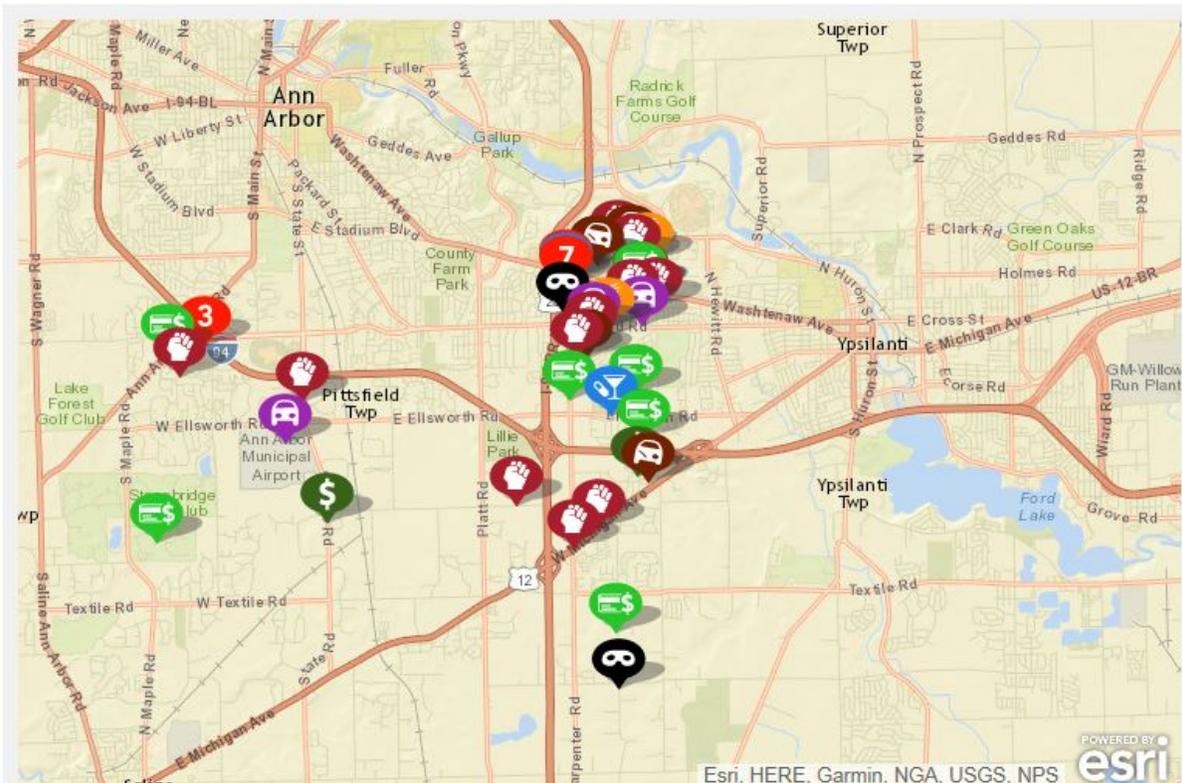## May 7th – 20th, 2017

"**_Click the image below for Two (2) Weeks of CrimeMapping details_**"

CrimeMapping.com Map- click on "show reports / print" for details.
May 7th – 20th, 2017, showing crime types: *Arson, Assault, Burglary, Disturbing the Peace, Drugs / Alcohol Violations, DUI, Fraud, Homicide, Motor Vehicle Theft, Robbery, Sex Crimes, Theft / Larceny, Vandalism, Vehicle Break-In / Theft, Weapons*

The below named incidents remain under investigation. If anyone has any information about or has been a witness to any of these crimes, please contact the Pittsfield Township Department of Public Safety at 734-822-4911 or the confidential tip line at 734-822 4959. Residents are encouraged to sign up for Pittsfield Township alerts and department notices through "_Notify Me_". Please go to www.pittsfield-mi.gov to sign up.

Gordon Schick
Deputy Chief of Police
(734) 822-4923
schickg@pittsfield-mi.gov

Sean Gleason
Fire Chief
(734) 822-4926
gleasons@pittsfield-mi.gov

Navigating the new Crime Mapping website for details

(To access information: √ -the Police badge, *under visible agencies*
√ - the box for the Pittsfield Twp. map, √ -show only records from this agency,-√ - on Reports for details)

CrimeMapping Alerts / Notices of "verified reported incidents" in your neighborhood:
This tool provides accurate information on "reported incidents" in real time from 500 ft. to 2 miles from your home. You can also access the Sex Offender's registry. Residents can get the alerts by email / text, today.
Sign up for crime alerts through **www.crimemapping.com** and for emergency notifications, including weekly public safety activity reports, at, www.pittsfield-mi.gov/notifyme

 Federal Trade Commission: Ransomware -WannaCry worries? Update now. By: Nat Wood | May 15, 2017

You've probably heard about the ransomware attack affecting organizations' computer systems around the world. Here's the best thing your company can do to avoid it: Update your operating system and other software. Now.

The ransomware, known as WannaCry or WannaCrypt, locks you out of your systems until you pay the crooks who installed it. It takes advantage of a security hole in Windows server software that can be closed by an update from Microsoft (link is external). Many of the organizations affected by the ransomware had not installed the software update.

If your company uses an older Windows network system no longer supported by Microsoft, you may not have been prompted to download security updates, but they're available from Microsoft's site (link is external).

Whether you manage a network or only have one computer, you should download security updates as soon as they are available – no matter what operating system you use. Hackers are constantly looking for security gaps, and companies try to close those gaps as soon as they are discovered. So it's important to download updates right away. Most operating systems have a setting to download and install security updates automatically. Use it. And install updates for your other software, including apps.

If you use old software that doesn't update automatically, set up a regular schedule to go to the company's website and download and install updates yourself – at least weekly.

In addition to keeping software up-to-date, here are a couple of other things you can do to prepare for a ransomware attack:
Back up your important files. From tax forms to planning documents, make it part of your routine to back up files often on your computers and mobile devices. When you're done, log out of the cloud and unplug external hard drives so hackers can't encrypt and lock your back-ups, too.
Think twice before clicking on links or downloading attachments and apps. Ransomware often is downloaded through phishing emails. You also can get ransomware from visiting a compromised site or through malicious online ads.

We've got more tips for keeping a small business's computers secure on our small business site, www.ftc.gov .