

# MEMORIAL VILLAGES POLICE

## CRIME ANALYSIS SUMMARY

January 3, 2014 through January 9, 2014

**FACEBOOK:** <https://www.facebook.com/mvpdtx>

**E-MAIL:** [mvpdtx@mvpdtx.org](mailto:mvpdtx@mvpdtx.org)

*For quick reference in reporting crimes or suspicious activity, program our dispatch number into the speed dial of your home and cellular telephone:*

**713-365-3700**

---

## CRIME ANALYSIS SUMMARY

### BUNKER HILL

On January 3<sup>rd</sup> an officer responded to a construction site on Rip Van Winkle for a construction material theft. The theft occurred between 01/02/2014 - 5:30 pm and 01/03/2014 - 8 am. This case is currently under investigation.

On January 3<sup>rd</sup> officers responded to a report of a suspicious vehicle on Greenbay. Officers located the vehicle and discovered marijuana in the vehicle. The driver and passenger were arrested for possession of marijuana.

### PINEY POINT

On January 3<sup>rd</sup> an officer was contacted by a resident on Tynebridge in reference to damage to their mailbox. The damage occurred on 01/03/2014 between 8:45 am - 1:30 pm.

### HUNTERS CREEK

On January 8<sup>th</sup> an officer responded to a residence on Hunters Creek Drive in reference to an attempted theft. The residence is under construction and unknown person attempted to gain access to the garage.

## CRIME PREVENTION TIPS

This holiday season, hackers stole over 40 million credit and debit card numbers from Target's retail system. This makes all of us extra cautious about protecting our own computer systems. Here's how to hold off those hackers:

**1. "ABC" online.** "Always Be Careful" when checking emails and surfing the Web. Hackers use these online connections to get malware onto your system that gives them access to personal information and passwords.

*Watch for bad links:* Check a link by resting your cursor on it, without clicking, to see the web address. If you want "Sports.com" but you see "x83pzt.net," don't click on it.

*Avoid questionable websites:* Places that push the norms of taste and morality are notorious sources of malware.

*Don't fall for phishing scams:* Wiring money to someone you don't know is never a good idea. But also watch for scams that pose as your bank, email provider, social media, or even the IRS. Banks don't ask to reset your password by email and the IRS never emails taxpayers.

*Don't download from an unknown source:* Only get files or apps from websites you trust.

**2. Use different passwords for different sites and accounts.** That way, if one account is hacked, only one is compromised. Write passwords down and keep in a secure place, or use a secure online password manager.

**3. Make passwords hard to hack and change them often.** "Password" and "123456" are easy to hack. So are your birthdate and your child's name, which can be found online. Experts suggest using a long sentence with numbers and symbols, such as "PumpkinsClimbIntoHurricanes%82&." Or make up an even longer sentence, such as "I came to Dallas in 2011 after living in Atlanta for 4 years", but just use the first letter of each word: "IctDi2011aliAf4y." And change passwords every six months.

**4. Watch what gets stored.** Never email your Social Security Number, because it stays in your archives. Delete old messages with bank account info or credit card numbers. Never put your master list of passwords on your computer.

**5. Use protection tools:**

*Antivirus software:* Scans for known computer viruses and some can detect phishing scams and other schemes.

*Secure connections:* If a website uses your personal info, make sure you're on a secure, encrypted connection. Instead of "http," the web page URL should start with "https"-the "s" stands for "secure."

**Two-factor authentication:** This makes sure no one can pose as you. Once you set it up, every login needs two steps. First, enter user name and password. Then you'll get a third, one-time password sent to your phone or other device. This option is offered by Amazon, Facebook, Google, Twitter, and others.

**What to do if you've been hacked?** Take these steps immediately:

- 1) **Destroy the computer virus:** Run antivirus software to find and remove the virus.
- 2) **Update all software:** Download the latest versions of all programs, including operating system, Internet browsers (Chrome, Firefox, Internet Explorer, Safari, etc.), Office, and Adobe programs.
- 3) **Change all passwords:** Make sure to do this on a different computer from the one that got infected. If the virus had key logging software, hackers might find the new passwords.

Mark Stokes

Detective

Memorial Villages Police Department

---

## Contact Information

City of Bunker Hill Village: 713-467-9762

[www.bunkerhill.net](http://www.bunkerhill.net)

Join Our Mailing List!