Vol 6, Issue 4

USAonwatch.org

February 15, 2016

# Woodlake Neighborhood Watch Newsletter

## MOSQUITO BORNE ZIKA VIRUS’ FIRST CASE IN HOUSTON:

The U.S. Centers for Disease Control and Prevention confirmed Houston's first case this month. A traveler returning from El Salvador in November fell ill with fever, rash and joint pain. The agency determined that she brought the illness into this country following a month of investigation and testing.

The mosquito-borne Zika virus that causes birth defects was identified Thursday as spreading explosively.

So far, cases have been reported in 23 countries.

The virus first identified in a monkey in the Zika forest of Uganda in 1947 has recently emerged with a vengeance in South and Central America, infecting millions. Zika is suspected in thousands of cases of microcephaly, a birth defect that causes newborns to have abnormally small heads and neurological complications.

About 1 in 5 people infected with Zika virus become mildly ill with symptoms similar to dengue and chikungunya: fever, rash, joint pain, or conjunctivitis (red eyes) and often muscle pain and headache that may last for a few days. The incubation period is from a few days to a week. The illness rarely requires hospitalization very few deaths are attributed to Zika.

The virus remains in the blood of an infected person for about a week, maybe longer in some people.

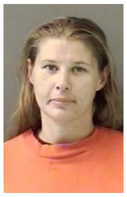
There is no vaccine to prevent or specific medicine to treat Zika infections. The best remedies are: get plenty of rest; drink fluids to prevent dehydration; take medicine such as acetaminophen (Tylenol®) to relieve fever and pain.

Do not take aspirin and other non-steroidal anti-inflammatory drugs. If you are taking medicine for another medical condition, talk to your healthcare provider before taking additional medication.

During the first week of infection, Zika virus can be found in the blood and passed from an infected person to a mosquito through mosquito bites. So, if you have Zika, prevent mosquito bites for the first week of your illness.

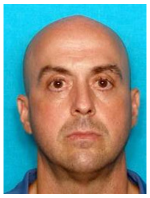
## COUNTY SHERIFF TIP LINE: WANTED AS OF JANUARY 15th, 2016

http://71.6.170.26/revize/ bellcounty/ departments/ cscd(adult_probation/most wanted.php , and/or; http://bellcountycrimestoppers.com;



Clarissa Renee Habib, from Temple, is wanted for: Unauthorized Use Of A Vehicle. Habib is a 30 y/o W/F with Hazel Eyes and Blond Hair who is 5’10” tall and weighs 253 lbs.

**FROM AUSTIN**: The reward for this month’s featured fugitive, Robert Chrismon, 53, has been increased to $8,000 for information received during the month of February.



Details:

- 5’ 5”, 180 lbs.,
- SMT: Scorpion tattoo on his right arm; scar on his chest; additional scars on both wrists.
- CCH: Parole violation: failure to comply with sex offender registration requirements.
- Ties to San Antonio, and he has been known to work as a general laborer.

Chrismon is a violent sex offender with a criminal history that includes aggravated rape, aggravated assault, kidnapping and escape.

In 1981, Chrismon was sentenced to 55 years for the kidnapping and aggravated rape of a San Antonio teenage girl. He received an additional 10 years for the attempted stabbing of a Corpus Christi police officer during an arrest.

For more information on the fugitives captured in 2015, see the captured fugitive archive at: http://www.dps.texas.gov/Texas10MostWanted/captured.aspx.

**All tips are guaranteed to be anonymous.**

## THE BEST DEFENSE AGAINST “RANSOMWARE” IS A GOOD OFFENCE.

**"Ransomware:"** Just the name alone lets you know it's bad news, but this type of virus is even worse than it sounds.

***Ransomware*** gets on your computer like any regular virus, such as through a phishing email or as a download from a sketchy website. However, unlike most modern viruses that stay quiet, you'll know it as soon as you have *Ransomware*.

A ***Ransomware*** virus immediately encrypts your documents, pictures, videos and any other personal files on your computer so you can't open them. The latest version of the CryptoWall ***Ransomware*** even scrambles file names so you don't know which files are which. The only sure way to get your computer back is to pay the creators a ransom, hence the name. Even the FBI has recommended people pay the ransom if they want their files.

The ransom can range from hundreds to thousands of dollars. Some viruses will raise the cost of the ransom over time to convince you to pay right away. At least one silver lining, if you want to call it that, is that paying the ransom usually does get you your files back.

Still, ***Ransomware*** is evolving rapidly and becoming more widespread. CryptoWall, TeslaCrypt, CoinVault and others have all appeared in exploit kits in 2015. Any criminal can buy a kit and launch advanced attacks against thousands or millions of computers.

That's why there's been a huge spike in ***Ransomware*** infections, and security experts expect that 2016 will be worse. Even with some security companies offering decryption tools for certain types of ***Ransomware*** like CoinVault and TeslaCrypt, the major players like CryptoWall are advancing too fast.

To avoid ***Ransomware*** in the first place is the best countermeasure, so here are 4 suggestions of how and what to do if it attacks you:

- Your best option to defeat ***Ransomware*** is to keep it off your computer in the first place. Security software is essential for this as it will block most attempts by hackers to slip viruses on to your system. If a virus does get downloaded, security software can often stop the virus before it causes too much damage.

There are several security software options and here are some suggestions; but it’s best that you choose the right one for your system and your budget. For example - Kaspersky Lab is the biggest security company in the world and a leader in identifying new security threats.

Their software can protect your computer against a lot of threats, but if your system is weak in certain areas then you might still be in trouble.

Keeping your operating system and Web browser up to date is also critical. Security holes in these areas can let hackers bypass your security software to slip files on to your system so keeping up with the latest updates for Windows, and how to make your Web browser hacker-proof.

Even with those areas updated, you still might not be safe. Be aware of phishing scams and how to avoid them. Also, learn how to spot disguised malicious files you might open without thinking twice.

- Even with all the security software,

*The publication of this newsletter is unofficial and does not express any opinion, directive, or policy of the Woodlake Property Owners Association members or Board of Directors. The primary purpose of the newsletter is to convey information designed to assist us to reduce or prevent crime in our community. The information presented is available through various public access sources, personal interview, or observation. Your comments as to how we can improve this effort are welcome.*

Vol 6, Issue 4

USAonwatch.org

February 15, 2016

# Woodlake Neighborhood Watch Newsletter

anti-virus and updated OS, what can you do if you still get ***Ransomware***?

The hackers have set-up a legitimate "Tech Support" to help you recover file after the ransom is paid. After all, if people couldn't reliably get their files back, then no one would pay the ransom.

However, before ***Ransomware*** can activate and encrypt your files, it has to "call home" first. This involves contacting a hacker-controlled server and getting a unique encryption key. This is what lets you decrypt your files when/if you've decided to pay the ransom.

It is possible to block the ***Ransomware*** from phoning home so it can't run by pulling the Internet cable as fast as you can or open a service called "OpenDNS".

This is a free service used to speed up the Internet while also blocking adult sites and other objectionable material on an entire network of 0computers and gadgets.

- What happens in a worst-case scenario of a ***Ransomware*** virus taking over your computer?

Security software from companies like Kapersky Lab can guard against older ***Ransomware*** such as TeslaCrypt, CoinVault or the original CryptoLocker, but the newer type of ***ransomware***, are more invasive so, you'll want to have a backup plan in place.

You should always have a backup; you never know when your computer might decide to crash.

Having copies of your important files means on an external drive, CD, SD, flash drive or an on-line service like "Carbonite" allows you to wipe your computer clean to get rid of the virus and start over without losing any of your important data. And, it will save you hundreds, if not thousands of dollars retrieving all that information if it's lost to ***Ransomware.***

**THE PROTECTIVE MEASURES MAY DIFFER, BUT THE OBJECTIVE IS THE SAME – You use firewalls** and passwords to protect your computer from hackers. You take the appropriate measures to prevent your car from being burglarized or stolen; but, when it comes to your home, have you taken all the precautions to protect it from invasion and burglary?

Sometimes you just have to think like a thief to evaluate how well your home is protected. That doesn't mean going online looking for a place to "fence" your valuables. Instead, take a good look at your home and the ways you would get in if you wanted to rob it. Those are the spots that deserve reinforcement and coverage from your security system – cameras and alarms.

If you're having a little trouble thinking on the wrong side of the law, keep reading because further on is some information about burglars and how they choose spots to break in. Having that information makes spotting your vulnerable spots easier and ideas of where to put protection in place.

There a many video and security systems to chose from. Finding the right combination depends on your budget, your crime risk and, of course, the desire for more piece-of-mind. Prices can range from a few hundred dollars like ***SimpliSafe***, that is a DITY project, or several thousand for a professionally installed system that is constantly monitored by a contracted agency.

For the novice, the DITY system that requires no drilling can be installed in as few as 15 minutes in any house, apartment or garage, is ideal. Some allow you to opt-out of expensive monitoring contracts or offer month-to-month deals that provide monitoring for only the times you're gone, or even better, you can monitor it yourself and call the police when you're alerted of a break-in. These systems complement having a trusted neighbor watch your place in your absence and taking advantage of the "Vacation Watch" program.

As promised here are some statistics to help put you in the mind of the burglar. According to surveys of actual break-ins, here are the parts of your home burglars are most likely to break in through:

- Front door - 34%
- First-floor windows - 23%
- Side doors - 22%
- Garage - 9%
- Basement - 4%
- Second-floor windows or doors - 2%

Here is the breakdown of why burglars would choose an area, what they looking for and how you can make it less attractive as an entry point. point.

The front door is the natural place to break in because a good burglar will make it look like they're walking into a home they own. Or if they're doing a quick smash and grab, most front doors can be kicked in with little trouble. You definitely want a motion sensor watching your front door no matter what. You should also install a high-quality deadbolt with a heavy-duty strike plate. That prevents the burglar from picking the lock or just kicking the door in. If your front door has a lot of glass, you might consider replacing it with one that's solid.

The reason burglars go for the first-floor windows next is that people usually leave them open at certain times of the year. Many windows also have bushes or trees covering them, so burglars can strike without being seen. Make sure that you have locks on these windows and that you remember to close them when you aren't home.

If your home windows are closed or easily visible to the street or neighbors, burglars will go for a less conspicuous side or back door. You can make these safer by putting a wooden or metal rod in the track to prevent it from opening. Then just make sure you have a glass-break sensor installed in case the burglar decides to smash it.

A garage door is actually easy to open, but then a burglar has to get through the inside door to get to the house. If you have a deadbolt on the inside door, most burglars won't even try it. And a motion sensor watching the door will catch the more tenacious ones.

If you're going out of town, you can padlock your garage door closed and make sure you aren't storing anything valuable in there. Consider installing a motion-activated light above garage door to stop burglars from sneaking up on it at night.

Be sure to padlock any exterior basement doors, and make sure the doors are very strong wood or metal. Attach the lock hardware securely so a burglar can't dislodge it with a kick. Then be sure to deadbolt the basement's interior door.

Despite what you see in many movies, most burglars are going to ignore second-floor entrances. These are harder to get to, and it's easier for someone to spot them breaking in.

However, if you have a second floor patio with a staircase, treat it like a first floor. Also, be sure not to leave any ladders around the yard, and trim back trees so a burglar can't reach windows by climbing.

Regardless, never leave a second-story window open when you leave the house. That will only serve as an invitation as a target to a burglar.

Now that you know how burglars think, give your house a good look-over. You might be surprised at some of the problems; if you can see a way in, can a burglar.

Fortunately, most problems are easy to fix. Having a good security system installed to alert you and the authorities when someone tries to break in cannot be over emphasized.

*(Source: KimKomando.Com)*

***The publication of this newsletter is unofficial and does not express any opinion, directive, or policy of the Woodlake Property Owners Association members or Board of Directors. The primary purpose of the newsletter is to convey information designed to assist us to reduce or prevent crime in our community. The information presented is available through various public access sources, personal interview, or observation. Your comments as to how we can improve this effort are welcome.***