Volume 4, Issue 1 January 1, 2014

Woodlake Property Owners Association Neighborhood Watch Newsletter

Happy New Year!

The publication of this newsletter is unofficial and does not reflect 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.

The Editor and Staff wish you and your loved ones a Very Happy and Fortuitous New Year. Please renew your resolution to stay safe and secure.

1. Bell County Sheriff Tip Line: Wanted as of December 30th, 2014 - http://71.6.170.26/revize/bellcounty/departments/cscd(adult_probation)/most_wanted.php , and/or http://www.golfkilleen.com/crimestoppers/wanted.htm; (No change) Three of this issue's infamous citizens hail from Killeen: Isaac Cabrera, 31, is a 160 lb, W/M with brown eyes and black hair, wanted for Assault Causing Bodily Injury; 36 y/o, 6'3", 150 lbs, Howard Rankin is wanted for Obstruction or Retaliation and; 4'11", 110 lbs, Tiana Newhouse, is a 23 y/o, B/F, wanted for Possession of a Controlled Substance. Also wanted for Possession of a Controlled Substance is 24 y/o Ashley Patton who is a 5'9", 154 lbs, W/F. Patton's last known address is in Temple.

Christopher Edgar is a 19 y/o, 5'4", 173 lbs, W/M, from Temple who is wanted for Unauthorized Use of a Vehicle.

Lastly, wanted for Injury to a Child, from Troy is 30 y/o Richard Allen. Allen is 5'9", 145 lbs.

Please review the attached flyer; if you have any information regarding those individuals; Call the Bell County Sheriff's Office at 254-933-5400, your local law enforcement, or CRIMESTOPPERS AT 1-800-729-TIPS (Local 526-TIPS) There is now an "on-line" crime reporting system for your convenience at:
http://71.6.170.26/revize/bellcounty/citizen_online_reporting_system/index.php

From Austin: An up to $10,000 reward is offered for information leading to the arrest of Raul Ambrosio Jimenez, Jr.; wanted for: Sexual Assault of a Child, Traffic of Person under 18 - Prostitution and Probation Violation (Original Offense: Manufacture/Delivery of Heroin). Race: Hispanic, Sex: M, DOB: 07/24/67, Ht: 5'9" WT: 210 lbs.

AKA: Rail Ambrosio Jimenez, Junior Jiminez, SMT: Tattoos: Female figure/scroll/ dragon on upper right arm; and male face/tower on upper left arm. Scar on left eyebrow. CCH: Prostitution, Burglary, Vehicle Theft, Counterfeiting, Possession of Marijuana, Resisting Officer, Manufacture/ Delivery of Controlled Substance, Traffic Violations. LKA: 7650 Highway 90, #813, San Antonio, Texas.

Details: Jimenez, is identified as a member of the Texas Syndicate gang from the San Antonio area and has relatives in the Bexar County vicinity. He has a lengthy criminal history dating back to 1987, with arrests for Prostitution, Burglary, Vehicle Theft, Counterfeiting, Possession of Marijuana, Resisting Officer, and traffic violations. In 2006, Jimenez was convicted of Manufacture/Delivery of Heroin, was sentenced to federal prison but was released with supervision 2011.

In November 2011, Jimenez was involved in the sexual assault of a female juvenile, resulting in a four-count indictment. On December 12, 2012, the Bexar County Sheriff's Office issued a warrant for his arrest for Sexual Assault of a Child, then in February 2013, the US Marshals issued a warrant for Jimenez's arrest for Probation Violation. Caution: Subject should be considered Armed and Dangerous!
Contact: **Texas Crime Stoppers** Text **"DPS plus your tip" to 274637** (CRIMES) or call **1-800-252-TIPS (8477)** - 24 hours a day.

2. Crime Update: **Fraudulent ID Used For Botox Treatment - Harker Heights** - Police are searching for a woman accused of stealing Botox treatment from About Face, located in the 200 block of E Central Texas Express, about 3 p.m. on October 22.

The woman described as a white female in her early to late 40's, with blond hair and brown eyes tried to pay for the $475 Botox treatment with a prepaid debit card, but it was not accepted.

She told the receptionist she would go to the bank and then come back and pay for it but never returned.

The identification the woman left with the business was, of course, phony.

Any person with information about this is asked to contact the Harker Heights Police Department, Criminal Investigation Division at 254-953-5400.

3. Part 1 of Our Cyber Crime Awareness Series; Cyberattacks and Ransomware. A Looming Real and Present Danger - As if the threat of access to all of our private information from every portal of the "Affordable Care Act" (AKA – Obamacare) Healthcare.gov, weren't bad enough, consumers across the globe are likely to witness more complex and diverse cyber-attacks in coming months.

Because high-volume advanced malware runs a higher risk of detection, cybercriminals will rely more heavily on lower volume, more targeted attacks to secure a foothold, steal user credentials and move unilaterally throughout infiltrated networks.

The prediction is that "Ransomware" will play a part in this trend and move down market to small- and medium-sized organizations with focused attacks on data stored in the cloud versus data stored on the network.

If your computer is infected with devastating "Ransomware", CryptoLocker will encrypt your documents then, if you want your files back, demand you pay a ransom that ranges from $100 to as high as $700 within 4 days.

However, the criminals behind CryptoLocker say that you can get them back even after four days but the price goes up to $2,000 or more! If you don't pay the criminals for their crime of locking your files using strong encryption, your files are permanently locked with very strong passcode.

While you might pay this ransom as a last resort, users are reporting that some files will give an error and stay locked, in which case, there is no way to recover those files.

Unfortunately, your antivirus software does not block this malicious virus.

This is important. If you get CryptoLocker, disconnect from your wired or wireless network immediately or else other systems on the network will become infected too.

Be sure to forward this security alert to your family and friends so they stay safe as well. This virus is hard to detect and is quickly spreading online.

Of course, your best option is to avoid CryptoLocker in the first place. That means avoiding malicious email attachments and downloads.

So far, it seems CryptoLocker arrives with fake UPS, DHL and FedEx emails as bait, so be on the lookout.

If you do accidentally download the CryptoLocker file, you want to make sure it doesn't run and cause damage. Most security software will only catch it after it's already running. At that point, it's too late.

You need a program that stops CryptoLocker before it runs. Fortunately, there is a simple program called CryptoPrevent that does just that and is available.

Of course, the person who makes CryptoLocker might change how it works. So, don't think you're totally safe.

The one sure way to keep your files safe is by having a backup.

Volume 4, Issue 1 January 1, 2014

Woodlake Property Owners Association Neighborhood Watch Newsletter

Happy New Year!

Even if you don't get CryptoLocker, there are other viruses and disasters waiting to take down your computer. Without a backup, your precious files will be long gone.

CryptoLocker is a sneaky program, so your security software might not get everything and cause problems in the future.

If you have the time and skill, you're better off wiping your computer and reinstalling everything.

In 2014, cyberattacks will be even more complex and diverse. While the general volume of advanced malware will decrease, it's expected that the volume of targeted attacks and data destruction incidents will increase.

Concurrent, class-based, object-oriented programming languages like *Java* will remain extremely exposed to exploitation as most end points will continue to run older versions.

As social networking continues to appeal to the business community in 2014, attackers will increasingly use professional websites, such as LinkedIn, to research and lure executives, to gather intelligence and to compromise networks.

Most major U.S. companies have been under siege from hackers over the last 18 months.

In fact, a hacker group called the Syrian Electronic Army has hacked the New York Times' website and Twitter feed twice this year.

Cyberattack isn't isolated to just businesses either. America's infrastructure: power grid, communications, banking and so forth are all at risk.

Every one of these services relies on computers. A well-placed virus could do a lot of damage, especially if an insider planted it.

The Northeast blackout of 2003 started at a single power center. A computer bug disabled an important alarm. The operators couldn't react in time to a downed power line and it blacked out 55 million people for several days.

Imagine waking up one morning with no power. Cellphones can't connect, banks are closed, the Internet is down and credit cards don't work.

In localized emergencies, workers from other areas help to restore services quickly. A cyberattack could affect wide regions of the country, overwhelming the available manpower, and take days, weeks or months for basic services to be fully restored.

Now, a cyberattack might not take down everything, but it could make basic services unreliable. You won't be able to trust technology to always work.

That's why you need a backup plan for your family. I would plan for at least 30 days of limited to nonexistent services.

Keep a supply of water and canned food on hand, along with a first aid kit. Knowing exactly what other survival tools to include can be difficult. Fortunately, the government has a site to help you plan your disaster kit.

Your emergency kit should contain cash. After all, debit and credit cards may not work.

Keep important documents within easy reach, too. You may not be able to get to documents stored on your computer. So, keep physical copies in a small safe near your disaster kit.

Being separated from your family is worrying, particularly in emergencies. So, your family needs to determine a gathering point. You might not have Facebook, Twitter or texting available to help you coordinate.

In a disaster, remember it's better to text than to voice call. Texts use less information so they don't overwhelm local cellular towers or use as much battery power as a phone call. Plus, texts can wait to send, so they'll still get through without your constant attention.

In localized disasters, it is often easier to contact people outside the area. So, designate an out-of-town relative as a contact person.

Don't count on cellphones to work properly either because, evident in Hurricane Sandy, cellular towers aren't as robust as traditional landlines.

Have one or more sets of two-way radios. They'll work in any situation. Be sure to choose a channel to use in advance. Choose a second one in case the first is in use. And be sure to stock up on batteries.

An AM/FM radio is another essential for any emergency kit. Radio stations have generators and can still keep broadcasting important information when other communication systems fail.

Choose a radio that can be powered by hand crank or solar power. Some can even charge other gadgets, like cellphones. Make sure the radio is capable of receiving NOAA weather alerts as well.

If you have young children, be sure to write instructions down for them. This can help if they're at school when disaster strikes.

For kids old enough to have a cellphone, make a note with the instructions and store it on their phone as a file or picture. Don't count on them remembering where to meet or what to do.

Whether or not a cyberattack ever happens, these are still good planning ideas. You never know when another kind of disaster might strike. A little preparation now might save your life - or a loved one's life - later.

4. On The Horizon - 4. On The Horizon - Part 2 of Our Cyber Crime Series; The 5 Internet Scams Designed to Rob You Blind - You probably know someone; have a family member, co-worker or friend whose checking account was emptied as a victim of identity theft.

Or maybe you yourself survived the heartbreak of nearly losing everything because of identity theft. Only recently debit and credit card numbers of more than 40 million in-store Target shoppers were swiped during the holiday shopping season.

Nobody is safe from identity theft but being forewarned is being forearmed, why you need to stay alert to the latest threats and be aware of the latest tricks identity thieves are using to steal your private information - and your money!

– *The WPOA NW Coordinator.*