Vol 6, Issue 9

May 1, 2016

USAonwatch.org

Woodlake Neighborhood Watch Newsletter

A CONFLUENCE OF "SEASONS"

In Texas, the demarcation between draught, wildfire, twister and flood seasons are seldom perceivable and, according to the National Oceanic and Atmospheric Admiration, flooding is the most common natural disaster in the United States. As we continue to witness the devastation in Houston, floods can happen anywhere and at any time, very quickly.

In March of this year, many residents not just in southeastern Texas, but also in parts of Louisiana had to evacuate their homes and communities to escape extensive flooding. FEMA recommends the following steps to protect yourself and your family against being trapped by floodwaters:

- Listen to local weather broadcasts and emergency alerts and, if authorities advise, evacuate before flooding starts
- However, if floodwaters cover the roadways around you, do not evacuate through floodwaters. Seek higher elevation instead.

If you see floodwater on roads, walkways, bridges, or elsewhere, do not attempt to cross. The depth of the water is not always obvious. Water may be covering a washed out roadbed or other hazards that may prove harmful.

Moving water has tremendous power. Six inches of moving water has the potential to knock an adult off their feet, and as little as one foot of water can sweep a vehicle off the road. Remember: Turn Around, Don't Drown!

Floodwaters can also contain hazardous materials, including rocks, mud, oil, gasoline, downed power lines, and even sewage. Be especially cautious at night when it is harder to recognize flood dangers.

The Storm Prediction Center is reminding people in general that it's late April and "twister" (tornado) season is here.

Yet, statistics show that with cooler temperatures and unpredictable, rapid changing conditions, results in uncertainty as to when to "raise the alarms".

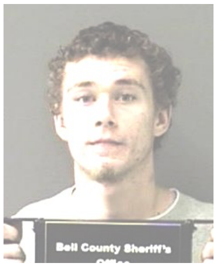
With too much notice, people might try to flee in their cars, putting them at greater risk. Too late or too little notice can result in destruction and broad casualties of whole communities.

This is why cleaning out the storm shelter and buying a weather radio, keeping some emergency provision available and lots of extra batteries is sound advice.

North Texas, and Oklahoma remain the most likely epicenter for severe outbreaks but the weather can change in an instant creating the disturbance necessary to spawn tornados and, like floods, just about anywhere, anytime.

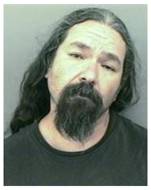
COUNTY SHERIFF TIP LINE: WANTED AS OF APRIL 30th, 2016

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



Mathew Helton, from Killeen, is a 22 y/o, White Male, weighing 140 lbs, is 6'1" tall with Blue Eyes and Blond Hair. Helton is Wanted For: Evading Arrest with a Motor Vehicle.

FROM AUSTIN – This despicable "low-life" character is Benjamin Dominguez and has been on the Texas "Most Wanted" list since 2000 or earlier. Dominguez is Wanted For: Indecency With a Child by Exposure, Probation violation (Original Offenses: Possession of a Controlled Substance; Resisting, Evading or Obstructing an Offer.



Details:

- White/Male, 5'7", 225 lbs.
- DOB: 10/30/66
- AKA: Francisco Rodriguez, Ben Dominguez, Francisco Dominguez, Rogelio Morales, Rogelio Lopez Morales, Rogelio Mendoza Morales, Rogelio Ramirez, Johnny Rodriguez, Roger Rodriguez, Francisco Sanchez, Javier Zuniga, Chino
- SMT: Tattoos: Skulls, scorpion, and prison on left arm; panther, female holding shotgun, and eagle on right arm; barbed wire on left wrist; and "Yvette" on neck. Scars on chin, left elbow, and finger(s) on right hand. Needle marks left arm.
- Gang(s): Barrio Azteca
- CCH: Indecency with a Child by Exposure, Failure to Comply with Sex Offender Registration, Assault Causes Bodily Injury, Possession of a Controlled Substance, Burglary, Failure to Identify-Giving False/Fictitious Info, and DWI.
- LKA: 10141 Kendrick Circle, El Paso, TX.

CAUTION: Subject Should Be Considered ARMED And DANGEROUS! For more information or updates in the event of his arrest, see his wanted bulletin at:**http://www.dps.texas.gov/Texas10MostWanted/SexOffenderDetails.aspx?id=326**.

THE THREE TOP SECURITY CYBER SECURITY THREATS THIS SUMMER

A leading tech-lab has announced that 34.2% of computer users experienced at least one Web attack in 2015. "Ransomeware" is attributed to infecting more than 750,000 personal computers; a number that continues to grow!

Statistics indicate that there are three major predominate threats we'll need to worry about: Data Breaches, Ransomeware and Browser Plug-ins.

RANSOMWARE ENCRYPTS YOUR FILES SO YOU CAN'T OPEN THEM, AND THE ONLY WAY TO GET THEM BACK IS TO PAY A RANSOM. EVEN THE FBI HAS ADVISED VICTIMS TO PAY, IF THEY WANT THEIR FILES BACK.

Most notable was the Targets' **data breach** of 110 million customers at the end of 2013.

With Hilton, Starwood and others experiencing attacks, by 2015 hotels became, and will continue to be the target of choice for theft of payment information by hackers.

Hackers will likely move on to more vulnerable targets as more retailers switch to point-of-sale terminals that work with the EMV chips in the newest credit cards and debit cards, and people start using mobile payment systems.

Hackers had their heydays in 2015 as over 100 million medical data breaches occurred. And, until insurance providers and other medical services are able to implement digital security measures, this trend will continue.

The basic rules of economics and supply and demand are driving the black market in medical information. In smaller supply than financial and personal information, hackers can sell your medical information for a higher price. Also, hackers can get more use from your insurance information for a longer period because most people pay more attention on their credit and bank statements.

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 9

USAonwatch.org

May 1, 2016

Woodlake Neighborhood Watch Newsletter

CryptoLocker arrived at the end of 2013 is probably the oldest known **"ransomware"** virus which is still a serious, growing threat.

Ransomware encrypts your files so you can't open them, and the only way to get them back is to pay a ransom. Even the FBI has advised victims to pay, if they want their files back.

Ransomware isn't just a worry for individual computers. It can lock up files on a network, which means one infection can bring down an entire company. It's also possible to get it on smartphones and tablets via a malicious text, email or app.

Ransomware can be avoided by not being lured-in by "phishing" emails with malicious links or downloads and backing-up your computer regularly. Some have gone so far as to keep all their working data on an external drive which is only opened when needed then, by closing and removing the external drive/card, you can easily wipe clean your hard drive if your PC is ever compromised.

It should come to no surprise that, since the average adult spends 20 hours a week online; most of which is spent in a Web browser, it is where hackers focus their efforts. If they can find a flaw in your browser, then they just need you to visit a malicious website to slip a virus on to your system.

Last year, hackers targeted a number of browser weaknesses, but by far the worst was Adobe Flash. There were times it seemed to have an endless string of emergency patches, with at least three instances in July and four instances between the end of September and the beginning of November.

IN TODAY'S CYBER CORNER...

FIVE TIPS FOR SAFE BROWSING:

(1) Keep Your Web Browser Up To Date - A lot of times, browsers like Microsoft's Edge, Mozilla's Firefox and Google Chrome issue patches and fixes for bugs they know about. Typically, they get most of them before hackers can have a field day exploiting vulnerabilities. Fortunately, most browsers like Firefox and Chrome have default settings for automatic updates.

Make sure you've got the latest version by opening the Menu icon (little box with three horizontal lines in the upper right corner of your page) then for example, choose "Help and About," select browser you normally use, then – "Settings", "Advanced Settings", then click or unclick "Protect You and Your Device From Dangerous Sites" to turn automatic updates on or off.

(2) Give yourself an extra layer of protection by **Uninstalling Unneeded Plug-Ins -** Even if your browser itself is secure, it might have third-party plug-ins that aren't. Java plug-ins have been riddled with security flaws. Most browsers have Java disabled by default now, but the new danger is Adobe Flash

Microsoft Silverlight, Unity or a toolbar that you installed years ago and don't actually need may also create unnecessary faults.

(3) Enable Click-To-Play Plug-Ins - Not every plug-in is one you want to get rid of, for example there are good reasons to keep Adobe Flash to run when you actually need it.

It's called click to play. Instead of a plug-in always running, you have to click on it to activate it.

To illustrate how this is done, in **Internet Explorer** go to the far top right corner, click on the little gear icon and choose "Manage Add-Ons." Highlight a specific plug-in in the "Toolbars and Extensions" area. If a plug-in is enabled, click the "Disable" button in the lower-right corner.

(4) Get Rid Of Unneeded Browser Extensions - Browser plug-ins and browser extensions are easy to confuse. Plug-ins handle video or other content that the browser can't handle on its own. Extensions are bits of code that add new features to the browser.

Extensions need your passwords to do their job. That opens up extensions to hackers, who use extensions to install malware.

So, before you install an extension, make sure it's coming from a trustworthy source and has been around for a while. Second, be sure to review your extensions every once in a while, to weed out the ones you don't need any more. If you're not using an extension, or you suspect it's not from a reliable company, delete it.

(5) Run Anti-Exploit Software - We always tell you to keep your devices safe with security software.

While most security software is great at detecting and stopping the millions of viruses out there before they can install, security holes in your browser and other programs give viruses a better chance to slip past unnoticed.

Software companies are starting to release anti-exploit programs. These watch your programs for signs that someone might be trying to use them to sneak on to your system. Then it blocks those attempts.

There are some free anti-exploit program you can try, for instance "Malwarebytes Anti-Exploit".

AND THEN (AGAIN) THERE'S FACEBOOK...

The responsible shopper would hesitate checking-out an interesting item with a very cheap price tag. However, one might think this is a legitimate good deal because of the millions of likes on Facebook, the great photos of all the products and, thought you've never heard of it, the page posts back to its site several times a day - so what's the problem?

A recent Buzzfeed report, some "Too Good To Be True" offers on Facebook are just that, and are causing some big problems.

What people thought they'd ordered and what they received were very different things and thousands have lost money on products far different than pictured in the glamorous photos.

Just like other phishing and online scams, the ads and websites look pretty legit. They use professional photos and slap security certificates on their site convincing even skeptical shoppers that the company seems legit.

The cheap product sales haven't seemed to harm the businesses. At least one of company made more than $200 million in sales in 2014. That e-commerce company was then acquired by one of China's biggest clothing companies.

Scams like this thrive, because enough people fall for them and often lose a lot more than just a few bucks.

But, with all the legitimate deals, discounts and money-saving opportunities available these days, how can you tell the good from the bad?

Here are a few clues to spotting the scam:

- If there are 0 negative reviews or comments.
- If you can't find a phone number or address for the company. If you do, go to their website to check it out.
- Then, confirm that the address/phone number of the company id real, and that the place exist.
- Check reviews and sources not recognized with the Better Business Bureau.
- Scams will often try to get you to act before thinking by creating a sense of urgency. Don't fall for it! Verify the legitimacy of the offer before submitting personal information.
- Before you enter your credit card information, confirm that the URL starts with "https"—the "s" stands for "secure"—and has a lock icon in the browser bar.
- Never purchase anything online with a debit card. A credit card will give you more protections if it ends up being a scam.

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.