Vol 6, Issue 6

March 15, 2016

Woodlake Neighborhood Watch Newsletter

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

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

Hollie Marie Stolp, 32, white female, weighing 180 lbs, standing 5'6", with Blue Eyes, Brown Hair, is Wanted For: Arson. Her last know address is in Temple.

FROM AUSTIN - The Texas Department of Public Safety (DPS) is asking for the public's help in solving the 2007 murder of Blase Wright Jr., 21, in Bexar County. As part of a DPS public awareness program, one unsolved case is featured by the Texas Ranger Unsolved Crimes Investigation Team each month in an effort to generate new investigative leads and bring added attention to unresolved or "cold cases" across the state.

On Feb. 2, 2007, Wright was in his Universal City apartment when he was fatally shot by an unknown person during an apparent burglary. A witness reported seeing a black male leave the apartment and enters a small gold car that was occupied by another black male and a Hispanic female, who was driving.

The Texas Rangers and investigators on the case would like to identify the Hispanic female driving the car. The forensic sketch (*above*) represents the woman's appearance at the time of the murder, and witnesses reported that she had reddish hair.

Investigators believe there are individuals who know who went to the apartment that day and why; and DPS is asking for anyone with information to come forward to help solve this crime. Individuals can submit a tip through the Texas Rangers' Cold Case website or contact the Missing Persons Clearinghouse at 1-800-346-3243. website at: http://www.dps.texas.gov/TexasRangers/UnsolvedHomicides/index.htm.

TAX SEASON IS OPEN SEASON FOR SCAMMERS AND CONS

Criminals will use any means, scamming and hacking, to take advantage of any opportunity to snag a mere fraction of the billions of dollars shuffled around between individuals, financial institutions and the government. And, tax season is their busiest time of the year, and why you can expect to encounter one or more scams in the next month meant to steal your information or money.

Here are three of the most common cons:

(1) Phone scams –A lot of people are on guard against scams on their computer, but they tend to be more trusting of people who call.

Scammers make it even more believable by spoofing caller ID to say "IRS" or to show a legitimate IRS number.

When you get the call, the "IRS agent" on the other end will claim that you have unpaid taxes. If you don't send them the money via wire transfer or prepaid debit card right away, they'll have the police arrest you.

In another variation, they might say that you have a refund you didn't know about and they need your bank account information to transfer the money. They might ask you to provide your Social Security number and other sensitive information to prove you're the right person.

The prospects of going to jail or getting more money are enough to fool every typically cautious people, especially when the IRS is involved. Fortunately, there are five ways you know that these calls are fake.

- The IRS will mail you an official bill on government stationery before it calls. If you do get a call, it shouldn't be a surprise.
- You can question or appeal the amount you owe before paying. There's no reason to rush.
- The IRS won't ask you to use a certain type of payment, such as insisting you use a wire transfer.
- The IRS won't ask for payment information over the phone, or any other sensitive information.
- The IRS won't threaten to have the local police come and arrest you for not paying.

If you aren't sure if you're being scammed, get the name of the person who called you and the branch they're calling from. You can also ask if there's a reference number for your case. Then go look up the phone number for that IRS office and call it directly. That should set the matter straight very quickly.

(2) Phishing email and text scams - You need to be extra careful at the moment because, according to the IRS, phishing emails have surged 400% this tax season. And it isn't just emails; hackers have also started sending more text messages claiming to be from the IRS.

The IRS says the emails and texts that hackers are sending include several messages, including: Update your filing details; Get your IP PIN; Get your E-file PIN; Order a transcript; and others. In other words, there isn't one just one red flag. The IRS also says the scams aren't limited to a specific area of the country.

Be extra careful if you receive an email or text where you're being asked to provide personal information, like your Social Security number. If hackers get their hands on this information, they may file tax returns in your name and collect a refund from the IRS.

Watch out for fraudsters slipping these official-looking emails into inboxes, trying to confuse people at the very time they work on their taxes. If you receive one of these don't open it, delete it.

The IRS generally does not initiate contact with taxpayers by email to request personal or financial information. You can report suspicious looking "phishing" emails to Phishing@IRS.gov.

(3) CEO scam – A medical company suffered a data breach when a scammer gained access to the CEO's email account and ordered an employee to send him a sensitive spreadsheet. This same tactic could happen in your business as well.

The tax season variant, which also happened, sees the fake CEO demanding all the employee W-2 forms be sent to them. Fortunately, the employee who got the email got suspicious and didn't send them.

One thing to look for is whether or not the request is coming from the CEO's official email address. Even if it is, it never hurts to double-check over the phone or in person if the request is out of character or is a lot of sensitive information.

(4) Another serious danger - Hacker may access you personal details from data breaches. Last month, identity thieves tried to use 464,000 stolen Social Security numbers to create E-File PINs on the IRS website. Not only would this help them more easily file fake tax returns, it would be keep the real taxpayers from filing theirs at all.

THREE MOST LIKELY CYBER THREAT FOR 2016.

According to the latest reports, 34.2% of computer users experienced at least one Web attack, and there were more than 750,000 computers infected with ransomware in 2015.

Vol 6, Issue 6

March 15, 2016

USAonwatch.org

Woodlake Neighborhood Watch Newsletter

Most of the threats break down into a few categories that can be guarded against.

The most common is **Data breaches.** From the massive 110 million Target customer breach at the end of 2013, this threat will continue for the foreseeable future.

Hotels, like Hilton and Starwood, were hackers' choice in 2015. However, as more retailers switch to point-of-sale terminals that work with the EMV chips in the latest credit and debit cards, and people start using mobile payment systems, hackers should move on to easier targets.

More than 100 million patient records were exposed in 2015, a problem that hospitals, insurance providers and other medical services will have to learn how to deal with.

The black market is flooded with stolen financial and personal information, which means your identity is selling for a few bucks, if even that. Medical information is in shorter supply, so hackers can sell it for more, and people are less likely to monitor their medical records as close as their credit and bank statements for signs of fraud.

A recent **breach at VTech**, a toy manufacturer, exposed information on more than 200,000 children, including their names, addresses and even photos. A data breach at Hello Kitty exposed information on 3.3 million users and high-tech toys that store information about kids and interact with them, like "Hello Barbie," could reveal a lot to hackers.

Ransomware will continue to be a serious concern in 2016, especially since hackers can now get it for free and modify it, as they want making it harder to combat.

Ransomware can lock up data files on an individual's computer, your smartphone or tablet via a malicious text, email or app. One ransomware infection can disrupt an entire network and bring down an entire company.

Fortunately, if you avoid falling for phishing emails with malicious links, you can keep it off your machine because ransomeware needs your help to download.

Take the extra precaution of backing up your computer files regularly, so if your files do get locked, you can wipe your drive and restore your files.

Lastly, **Browser plug-ins** are exploited by hackers to find flaws or for you to visit a malicious website for them to slip a virus on to your system.

It should come to no surprise that's where hackers focus their efforts because adults spend an average of 20 hours a week online, Web surfing.

Learn how to spot a malicious site before it's too late. By far the worst is 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.

Because many online ads use Flash, even legitimate sites could infect a computer if hackers got an ad network to run a malicious ad.

While companies are quickly moving away from Flash, Facebook for example just switched its video player to HTML5, Flash isn't going anywhere for a while. In fact, just like Java, which was the security nightmare before it, Flash could hang around on computers for years after people no longer need it.

You can expect to see plenty more attacks against it this year. And hackers are probably already probing for the next big hole in browser security.

FIVE REASONS YOUR HOME MAY BE TARGETED BY BURGLARS

Burglary is a crime of opportunity. Which means that would-be thieves aren't spending a lot of time "casing-out" your home, or spend a lot of time planning-out their "capers".

Instead, a burglar will be walking or driving by, see an immediate opportunity and take it to swipe as much of your stuff as possible. If there is planning, it revolves around picking up clues as to when no one is home.

A burglary can happen at any time, but that doesn't mean there's nothing that can be done to make your home a less appealing target for thieves that'll motivate them to go off in search of an easier target.

What are some common mistakes you need to avoid?

(1) Leaving your garage door open - An open garage door is generally a sign that someone is home. However, a criminal walking by gets to see exactly what's in your garage, and whether there's a lock on the inside door. They might swipe something right then or plan to come back later.

If you've left both your garage door and inside door open, and you aren't in view, an especially bold thief might just walk into your home to see what they can take. According to the FBI, 33% of burglaries are unlawful entries, which means no force was used to enter the home.

Keep your garage door closed as much as possible to avoid tempting thieves to strike, especially if you aren't visible outside.

(2) No motion sensors/outdoor lighting - Thieves love the dark because they can more easily sneak up on a house without neighbors or passersby spotting them. Few thieves are going to waltz up to a house with exterior lighting showing their every move.

Of course, you don't want outdoor lights on all night, which is why a motion sensor is a good compromise. If a criminal tries to creep up at night, the light comes on and they'll think twice about going further.

(3) No interior lights - While some burglars don't have a problem robbing homes with people present, most of them prefer empty houses. In fact, according to the Bureau of Justice, less than 28% of burglaries happen when the homeowner is present.

Just be advised that in nearly two-thirds of cases where someone is home and the burglary turns violent, the burglar and the homeowner know each other. Fortunately, violence only occurs in 7% of all household burglaries.

While some people think the solution is turning on an interior light when you aren't home, that only works for so long. If you're on vacation, having a light on 24/7 is a giveaway that someone isn't really home. A burglar walking by several times or for several days will catch on fairly fast.

Putting multiple indoor lights on timers is better as they mimic someone moving around the house, or turning the lights off for bedtime. Another option is using lighting that is designed to mimic a TV being on. These have built-in light sensors and timers to better create the illusion that someone is watching TV during typical TV viewing hours.

(4) Overgrown landscaping - Just like burglars prefer dark to sneak up on a house, your landscaping can make it easier for them. If you have high bushes surrounding the front door or windows, burglars can break in and no one from the street can see them.

Keeping bushes low and your yard fairly clear means burglars aren't going to have any hiding places. If you have a second floor, trees near the house could also provide a way to get to the second floor, where people are less likely to lock windows or balcony doors.

(5) No security system – Even if a burglar isn't scared off by the exterior lights, lack of cover and interior lights, they'll run when an alarm starts blaring and why having a home security system installed is wise.