Vol 6, Issue 23

December 1, 2016

Woodlake Neighborhood Watch Newsletter
Holiday Edition

HOLIDAY SHOPPING SURVIVAL TIPS

Can you believe it!? Thanksgiving is gone and Christmas is "just around the corner". The Holidays ARE HERE and so is the rush to find that "perfect" last minute gift or, even more stress-related, hours online wishing you'd started on Halloween for your thoughtful gift to get to its destination on time. It's estimated that shoppers will spend close to $45 billion online this year. The caveat? With so much personal financial information out there, instances of identity theft are going to increase precipitously.

Anyone who shops online is vulnerable to having their identity compromised. The proper precautions combined with identity theft protection are your strongest safeguards in protecting your credit and preventing the financial ruin that can be caused when an identity is stolen.

These are some holiday shopping safety tips that offer you some on-line protection:

• Shop Trusted Names like Amazon.com, Target.com or other familiar retailers. Beware of ways scammers trick consumers by misspelling domain names using ".net" instead of ".com".

• Look for the Lock of secure websites that start with https:// instead of http://. Secure sites will also have a small lock icon in the lower-right corner of the screen. Never give anyone your credit card through email. PayPal, however, is still a good, safe way to make a payment.

• Don't Share Too Much is an extremely important online shopping safety tip. Keep your personal information protected from stores because they don't need your social security number or your birthday; in the hands of the wrong person, combined with your credit card number, serious damage can be done.

• Check Billing Statements for credit and debit cards as well as checking accounts regularly. If you see any charges you don't recognize,

• address the matter immediately. Don't pay credit card bills until you know all your charges are accurate. You have 30 days to notify the bank or card issuer of problems. After that, you might be liable for the charges.

• Use Stronger Passwords for each of your many online accounts—banking, credit cards, email. Often simple passwords that can be easily recalled are recycled, easily cracked and exploited. Use uncrack-able passwords, especially when banking and shopping. Avoid: using numbers or letters in the order they appear on the keyboard ("1234" or "qwerty"); your child's, pet's or name of your favorite team, or city of birth; your birthday, anniversary, date of graduation, or car license plate number; or common phrases like "letmein," or, especially, "password."

• Think Mobile by avoiding the temptation to brows online with your smartphone to find gifts. Instead, download store-specific apps like those for Amazon.com and make your purchase without going to their website.

• Stay at Home from where you can do most holiday shopping safely and securely. Doing all your online shopping at home is beneficial because you know that your purchases are being made on a trusted, secure network.

• Enroll in an Identity Theft Protection Service to help protect you from identity theft. Having a service provider you trust is important for identifying and remedying any fraud issues.

By following these simple holiday shopping safety tips and preparing for the worst, you can help to ensure your family—and your property—remain safe year-round. (Source: www.protection1.com/resources/online-shopping-safety)

HOLIDAY SAFE-SHOPPING TIPS REFRESHER

Never leave their purses or wallets unattended while shopping. Especially during the Holiday Season, criminals will be looking for the opportunity to victimize individuals that do not take precautions to minimize their risk of theft.

• Only carry a minimal amount of credit cards when out shopping.

• Do not carry your Social Security Card or PIN numbers in your wallet or purse. Leave these items in a secure place at home.

• Taking the extra time to close your purse and keep it with you while shopping or in public places will reduce the opportunity for thieves to take wallets and other valuables.

• Do not leave your purse or other valuables in plain sight unattended in your vehicle. Secure them in the trunk.

• When possible walk to your car with someone or ask a store employee to walk with you to your car especially after dark.

Individuals who are victims of purse / wallet theft or credit card theft should make a police report and contact their credit card companies to cancel the card and contact the three major credit reporting bureaus to place a fraud alert on the cards. For more information on Identity Theft and Credit Card Theft, contact your local Police Department or Sheriff's Office or the Federal Trade Commission at http://www.ftc.gov/.

LIKE SOCIAL SECURITY, KEEP CELL NUMBERS SECURE

We've learned that our Social Security number (SSN) is something that we shouldn't give out to just anyone because it can easily be used for frauc and identity theft purposes.

Besides used to contact you, your cell phone number is also used by many companies, including financial institutions and social networking sites, as a link to your private information.

The difference is that Social Security numbers are regulated and companies are required by law to keep them private. Cellphone numbers, however, are not and people tend to give them out without thinking of it as a security risk.

A government study shows that almost half of all U.S. households no longer have landlines, and the number of households with only wireless

Vol 6, Issue 23

December 1, 2016

Woodlake Neighborhood Watch Newsletter
Holiday Edition

phone service has been increasing steadily over the last few years.

It's possible that someone who grows up in a house with no landline, has never heard of a "rotary phone", could have the same cellphone number their entire life and be vulnerable at a much higher risk.

Because cell numbers are linked to many databases and are connected to devices that are almost always readily available, cellphone numbers could be more valuable to a cybercriminal than Social Security numbers.

Criminals looking to steal someone's identity or commit fraud have always tried getting a hold of the victim's Social Security number, which have become a universal identifier. Cybercriminals targeted large storage databases held by corporations, hospitals and government agencies looking for new identity theft victims.

But, as security got tighter, scammers are now trending toward the more lucrative target of cellphone numbers.

What are some things you can do?

- **Be cautious** about giving your cell number to anyone of questionable trustworthiness.
- **Use two-factor verification** that sends a security code SMS to your smartphone whenever someone tries to log into one of your accounts from an unknown device. This code, together with your password, will add extra layers of security to your account.
- **Check your credit report** on a regular basis. This can tip you off if you are a victim of identity fraud. Make sure there are no credit accounts under your name that you did not open.
- **Keep track of your bank accounts** for any suspicious activity and if you do find it, report it to your financial institution immediately.

BELL COUNTY WANTED AS OF: DECEMBER 1, 2016

Leighanne Marie, 24, is a B/F with Brown Eyes and Black Hair from Temple. Marie stands 5' tall, is 205 lbs., and is Wanted For: Burglary of a Habitation with Intent to Commit Theft.

FROM AUSTIN – The reward for information leading to the arrest of: **Guillermo Chavez,** has been increased to $5,000.

WANTED FOR: Probation Violation, Failure to register as a Sex Offender, DWI

DETAILS: W/M, DOB: 03/29/69, HT: 5'7", WT: 130 lbs. SMT: Scar on chest, AKA: Guillermo Chavez-Gonzalez, Guillermo Gonzalez, Guillermo Rosales, CCH: Aggravated Sexual Assault, Indecency with a Child, Driving Under the Influence-Liquor, Driving While Intoxicated LKA: 3925 Mountain Avenue, El Paso, TX CAUTION: Subject should be considered ARMED and DANGEROUS!

Born in Chihuahua, Mexico, when 14 Chavez moved to El Paso.

In 1998, Chavez was arrested for sexual assault on a 6 y/o child over a period of four years. During the investigation, a second victim Chavez had sexually assaulted was discovered.

On September 6, 2001, he was found guilty of three counts of Aggravated Sexual Assault of a Child and two counts of Indecency with a Child.

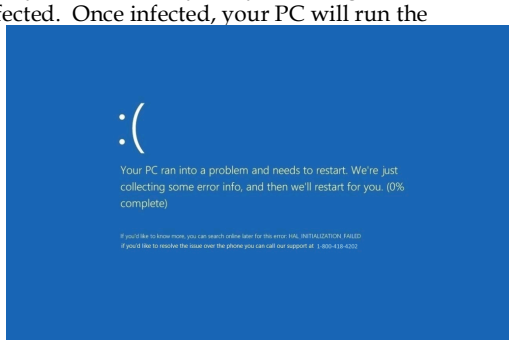
Before he disappeared in '02, Chavez was paroled and as required, renewed his driver license.

In December 02, a warrant for Chavez's arrest for Aggravated Sexual Assault and Indecency with a Child was issued.

www.dps.texas.gov/Texas10MostWanted/SexOffenderDetails.aspx?id=338

WARNING!

There is malware called Hicurdismos that targets Windows OS. Even if you're running Microsoft Security Essentials or Windows Defender, you still might be vulnerable. This malware threat is actually an installer that arrives by drive-by-download. If you try installing the fake Microsoft Security Essentials, your PC will be infected. Once infected, your PC will run the Hicurdismos malware and display a fake Blue Screen of Death (BSOD, at right), which denies access to the mouse, disables Task Manager, and displays fake BSOD preventing the user from using the PC.



If you call the fake tech support, scammers will answer the phone and try to steal your money by trying to convince you that there are more problems with your PC and you need to pay them for their services or software to fix the problems. The scammer might also try to get you to download more malware disguised as support tools to fix the problem, that doesn't actually exist.

Real error messages from Microsoft will not include a phone number for support. They will actually provide you with an error code and instructions to search for more information. Windows 8 and 10 already has Windows Defender built-in, so there is no need to install Security Essentials. Check certificates that are signed by Microsoft installers. (Source: KimKomando.com)