

Quarterly Community Newsletter

JANUARY 2012

NEW YEAR ALERT

It's a new year. For some people it's the winter season, for others it's the tax season and still others call it their golden season. All are correct. The winter season began on December 21, last year and it will end on March 21st. The tax season began on January 1, 2012 and will end on April 15, 2012. And, for identity thieves, the golden season is another name for the tax season because they harvest tax information from others for their benefit. This is not new. It's the same old dangerous scam in a new year, but people forget. So, we'd like to remind you of some safety procedures you can use to protect yourself and your family.

BACKGROUND INFORMATION

January is the prime time for a once-a-year opportunity for ID thieves. Beginning in January businesses like banks and other organizations (like your employer) begin to calculate our income received and taxes paid last year. They post this data on documents such as W-2 forms and/or 1099 forms. These and other forms contain detailed, sensitive information, including our Social Security numbers. Once completed the forms are placed in the U.S. Mail and then delivered to our own mail boxes. We have heard that in January through February, ID thieves can and will follow postal carriers who will fill our mail boxes with envelopes containing our personal, private tax information and then, when the carriers are out-of-sight, they help themselves to our mail.

PROTECTING YOUR INCOMING MAIL

Following are some suggestions and ideas that may protect your incoming mail.

1. Some experts recommend you rent a Post Office Box to collect your sensitive mail. It's a bit late for that this year, however if you rent a box now, immediately notify all your sensitive information providers of your Post Office Box address.
2. Install a locking mail box at your home, or if possible, add a lock to your existing mail box.

3. Or, pick up your incoming mail as quickly as possible after it is delivered. If you are not home at the time your mail is delivered, perhaps you can ask a trusted neighbor, family member or friend to pick up your mail for you.
4. If you'll be leaving town on business or going on vacation it would be a good idea to request your mail be held at your Post Office until you return.
5. Keep track of all the tax information documents you are expecting to receive. If the documents do not arrive, call the sender and report your missing documents.

ON-LINE IRS EMAILS, FAXES OR PHONE CALLS.

All through the tax season you can expect bogus emails and occasional faxes or phone calls from people who say they represent the Internal Revenue Service (IRS). Claims ranging from checking out past problems on your tax forms – to “new” information you must receive, are intended to make you share your personal information. **THE IRS WILL NOT SEND YOU EMAILS, FAXES OR PHONE YOU TO REQUEST PERSONAL, PRIVATE INFORMATION.** If the IRS has legitimate inquires to make from you, the inquires will come through the U.S. Mail. You can verify the authenticity of what has been received by calling: 1-800-829-1040.

MORE TIPS TO PROTECT YOURSELF DURING TAX TIME.

As the tax season continues there are more doors we can open to ID thieves – following are some tips to protect yours:

1. As you compile your data for the tax forms, you may go through and review all the paper work you've collected throughout the year (or years past) – remember, we only need to keep seven (7) years of tax documents. If you decide to throw away any documents containing financial, personal, sensitive information you no longer need, do not just throw it in the trash. Even in the age of internet, the majority of ID theft still takes place in low-tech ways – like shifting through garbage for discarded statements and receipts. Consider shredding your documents before you put them in your trash.
2. When choosing a tax filing service, select someone you know, or know about. Ask your family or friends for their recommendations. Avoid temporary store front services. If something goes wrong and they do not do the correct things for you, they will not be available when you need them. The IRS provides a list of approved Tax Service companies at www.irs.gov/efile.

3. If you use your personal computer to prepare your taxes:
 - a. Make sure your computer is protected with an updated firewall and secure software systems which contain antivirus and anti-spy software programs.
 - b. If you are storing important tax related documents on your computer, change your password frequently between December and April.
 - c. Make sure every web site you are using during the tax season is encrypted to protect your personal information when transmitted.
4. We recommend you do not mail cash to pay your bills.
5. When you are ready to write your checks to pay your taxes:
 - a. Remember, do not use initials for the name of agencies. Example: We used to be able to write our checks payable to the Internal Revenue Service as *IRS*. It was learned that IRS could easily be changed to MRS and a last name added to the check. So, now we are required to address our IRS checks as payable to the United States Treasury.
 - b. Consider always using a liquid ink pen when writing any check. Liquid ink penetrates the paper of the check and is more difficult to remove than ball point pen ink.
6. When you are ready to mail your tax forms we highly recommend taking the envelope directly to a post office near you. And, we recommend you skip using the blue Postal Collection boxes located on streets.

Last year in April, for the first time in our town, thieves ripped two (on different days) blue mail boxes out of the concrete and stole all the mail inside them. The empty boxes were later found south of Highway 74, near Homeland. None of the mail was ever recovered.

7. If you must do your mailing from home, make sure the tax forms, backup documents and enclosed checks are not visible from the outside. Try wrapping your forms in an extra sheet of paper to disguise the contents of the envelope. **DO NOT PUT THE MAIL BOX FLAG UP.** This only alerts identity thieves there may be an outgoing check in the mail.
8. Keep all your tax paperwork and all other private, personal, and financial documents in a safe and accessible place – such as a fireproof box, carefully secured in your home, but not in the master bedroom.

TARGET HARDEN YOUR I.D.

Not long ago, I.D. theft was the fastest rising crime in the world. Millions and millions of people were (and are) victimized when someone stole their I.D. and used it for their own benefit. I.D. theft is still huge – but it has slowed down some due to better safeguards financial institutions have put in place and because eagle-eyed consumers (you and I) are doing a better job watching over our accounts. That doesn't mean we no longer have to be alert and aware of protecting our financial and personal information. More than 500 million identity records have been lost or stolen in the United States since 2005 – through data breaches at businesses, government agencies and other organizations. That means we need to continue to focus on ways to protect ourselves. Following is a review and update on what you can do to prevent I.D. Theft.

WHAT YOU CAN DO TO PREVENT I.D. THEFT.

There are many ways crooks can steal your I.D. First, you should know you cannot totally shield your I.D. Some things are out of our control. If a crook really wants something you have, they will find a way to get it. However, sometimes you can make getting what you have so difficult to get (target harden), the crook will look elsewhere for an easier target. Some good target hardening rules are:

1. Be stingy with all your personal and private information. Safeguard it. Never give personal and private information to anyone until you have determined the requestor has a right to know. Never verify any information by telephone unless you made the call. Always ask for Privacy Policies. Then ask how the requestor will store and/or discard your personal information when the transaction is completed. You don't want documents or records containing your name, address, Social Security number, birth date, account numbers, or driver's license number to end up in someone's dumpster or unguarded data base. Bad guys look in these.
2. Travel lightly. Do not regularly carry your Social Security card, birth certificate, extra credit cards or check book unless you plan to use them today. Clean out your wallet. Carry only what you actually use today or must have in your possession. Then, using a copy machine, copy the front and back sides of everything you are carrying in your wallet. Keep the photo copy at home. If you should lose your wallet, you will be able to report exactly what it was you were carrying.
3. Cancel what you do not use or need. If you are not using a particular credit card, notify the issuer and cancel the account. Simply cutting up a card does not cancel the account. The number still exists for crooks to use.

4. Think of pre-approved credit offers as I.D. theft waiting to happen. Consider removing your name from the credit card prescreening programs at the three major credit reporting bureaus by phoning: 1-888-567-8688 or on-line at www.optoutprescreen.com One message will notify all three major credit bureaus.
5. Keep your mail box locked or pick up your incoming U.S. Mail shortly after it is delivered. Open and inspect all your mail. There is no such thing as junk mail. All mail is important. If you do not wish to take advantage of what is being offered, physically remove your name and address from the offer before you recycle it. Simply marking out your name with a marker is not good enough – tear it out, cut it out, shred it or burn it in your fireplace. Bad guys love our recycle trash barrel.
6. Outgoing mail containing checks should be hand carried directly into a Post Office.
7. Always check your monthly statements against your receipts and look for charges you did not make. This is the best way of making sure no one is using your credit card numbers. Also check utility bills for unusual charges. If you see something wrong, contact the agency immediately to make corrections.
8. When disposing of any documents, receipts, records or statements such as: canceled checks, utility bills, bank statements, credit card, medical or broker statements, tear, cut or shred them into small bits.
9. It's a good idea to check your one free credit report each year. We suggest you ask for one of the companies report – every 3-4 months – as a way to cover your review all year long. The three national credit reporting agencies are named Equifax, Experian and Trans Union. Congress passed a law to make it easier to obtain these reports by contacting any of the three agencies, using a single address and stating which company you want your report from this time.

Web: www.annualcreditreport.com

Phone: 1-877-322-8228

Post: U.S. Mail Annual Credit Report Request Services
P.O. Box 105281, Atlanta GA 30348-5281

10. If you have a home computer, you might want to consider installing/updating firewall and virus detection software. Be sure to log off when finished and turn off the power to discourage hackers. If you are discarding your old computer, you may want to destroy C.D.s or floppy disks containing sensitive data by shredding, cutting, or breaking them. Use hard drive shredding software or remove and destroy your hard drive before discarding a computer. Just deleting files is not good enough.

IF YOU BECOME A VICTIM

- 1) Start a diary. Record everything you do. Record who you contact, when, where, and what was accomplished. You will need this information if you take the criminal to court.
- 2) File a crime report with the Hemet Police Department.
- 3) Notify the credit card issuer, bank, creditor, utility or other agency where the theft occurred. Close all accounts used by the thieves. Choose all new passwords and pin numbers. Do not use your mother's maiden name as a password.
- 4) Alert the credit reporting agencies. Contact: Equifax at 1-800-525-6285 or www.equifax.com; Experian at 1-888-397-3742 or www.experian.com; and Trans Union at 1-800-680-7289, or www.transunion.com. Ask to have your account flagged with a fraud alert. By law, the agency you contact must alert the others. Ask them to put a fraud alert on your credit report. Doing so can help stop people from opening new credit accounts in your name.
- 5) File a complaint with the Federal Trade Commission, 1-877-438-4338, 1-202-326-2502 (TDD) or www.ftc.gov/bcp/edu/microsites/idtheft.
- 6) If you think the fraud involved your U.S. Mail – contact the local post office.
- 7) If you think the fraud involved your Social Security number – visit the local Social Security Office.
- 8) Expect to hire your own private attorney and do most of the investigating yourself.

REDUCING JUNK MAIL

First, there is no such thing as junk mail. If it has your name on it – it's important. We encourage you to open all incoming U.S. mail with your name on it. If you do not wish to take advantage of what is being offered – we encourage you to remove your name from the mail so no one else can use it. To remove your name: tear it off, cut it off, use a shredder, or use your fireplace. Simply crossing your name out with a pen or pencil just isn't good enough these days. If you'd like to reduce the volume of your national advertising mail – we suggest you contact the Direct Marketing Association (D.M.A.) the D.M.A. is the oldest and largest trade association with over 3,000 direct mail firms, catalogs, publishers, retailers and service organization members. D.M.A. has agreed, if you ask and pay \$1, they will allow you to opt out of their mailing lists. Simply fill in the form below, enclose your check or money order, and mail it to them. Or opt out online: www.dmaconsumers.org/cgi/offmailinglist. There is a \$1 fee, payable by credit card.

Date:

To the Mail Preference Service:

Please remove my name and address from the Mail Preference Service Mailing list.

Name: _____

Address, Apt.#: _____

City, State, Zip: _____

Thank You

(Signature)

Enclosed: My ___ check or ___ Money Order for \$1.

Mail to: Mail Preference Service Direct Marketing Association
 P.O. Box 282, Carmel, NY 10512

HOW TO KEEP YOUR NEIGHBORHOOD WATCH ALIVE

Initially, a Neighborhood Watch group is usually formed in response to crime or some kind of problem. But when the problem is solved or the crisis has passed, the Neighborhood Watch programs sometimes fade. So, how do you keep the neighbors interested? Here are a few suggestions.

1. Keep information and communication flowing between Hemet Police and among your neighbors. Sharing this newsletter can help you with this.
2. Or produce a newsletter for your group and include information about your neighborhood other than crime news.
3. Follow planning and zoning issues that may affect your area.
4. Host neighborhood events such as pot lucks, block parties, garage sales, and holiday events (a New Years Eve Party?)

5. Organize activities like neighborhood clean-ups and youth projects to keep youngsters busy and learning. Cleaning a neighborhood helps the looks of your streets and can stop or slow decline and decay. Crime breeds and grows in areas without the appearance that owners care. Clean neighborhoods retain their property values better. These activities encourage citizens to interact and feel ownership within the neighborhood, not just their own homes. This makes a neighborhood a "community", not just a cluster or row of houses or apartments.

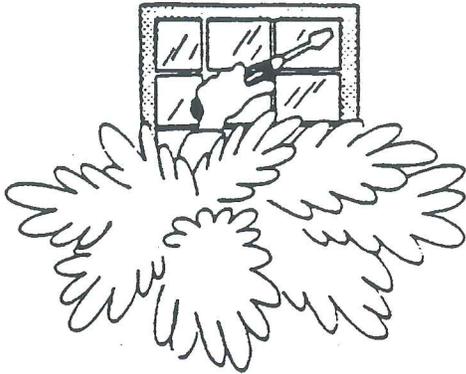
SOME FACTS.

- Working programs reduce crime as much as 80%. According to criminals, watch programs scare them into other neighborhoods.
- Burglaries, auto thefts, rape and child abductions and arson are the most prevalent crimes.
- Household burglaries are one of the easiest crimes to commit and prevent...but one of the hardest to solve.
- More than half of police time is spent investigating burglaries.
- Statistics show that in more than half of household burglaries, forced entry is not involved.
- Most household burglaries occur during daylight hours.

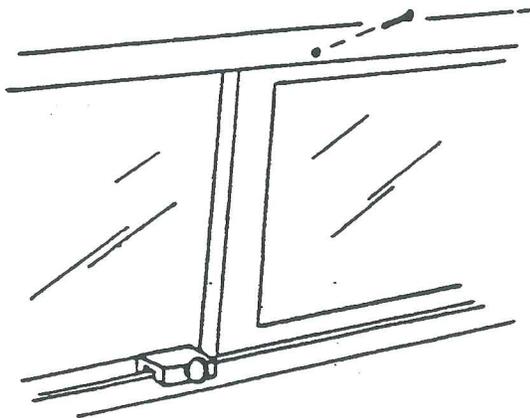
**If you wish to be removed from our mailing list, please call 951-765-2415.
If leaving a message: Please speak slowly, spell your name and repeat your phone number.**

HEMET POLICE WANTS TO HEAR FROM YOU		
YOU HAVE A QUESTION? WE HAVE ANSWERS		
Send your comments, suggestions, questions, or just interesting thoughts to the Hemet Police Department. We might even publish them in a future edition of the Quarterly Newsletter. Reach us at:		
Hemet Police Department Neighborhood Watch, R. Moyer 450 East Latham Avenue Hemet, CA 92543		
Phone (951) 765-2415	E-Mail rmoyer@cityofhemet.org	Fax (951) 765-2412

WINDOW SECURITY

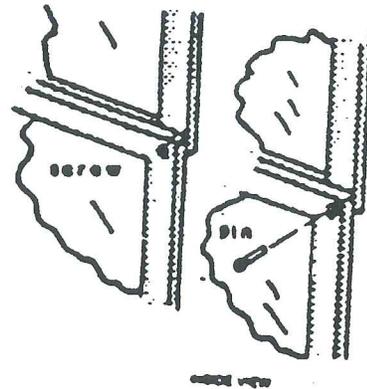


SHRUBBERY should not conceal any potential criminal entry points. It should be trimmed so that it does not conceal any portion of the window.

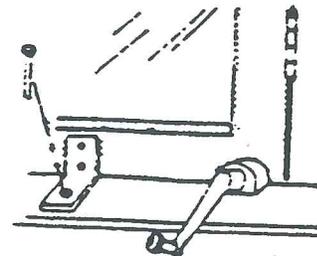


ALUMINUM SLIDING WINDOWS can be lifted up and out of the track. If possible, drill a hole through the inside window track and halfway through the window frame. Insert a steel pin or nail (see diagram). In addition, an anti-slide block can be used at the base of the window to keep it from being opened.

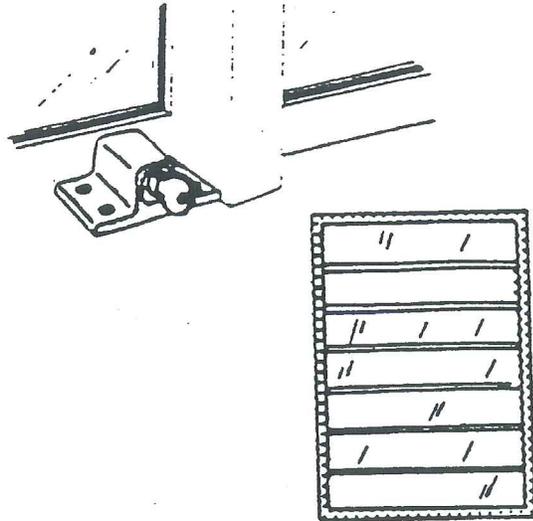
DOUBLE HUNG SASH TYPE WINDOWS (which operate upward and downward) usually possess a standard locking device which can easily be jimmed open. Install a good quality additional locking device or drill a downward sloping hole into the top of the bottom window through and into the bottom of the top window. Insert a steel pin, bolt or heavy nail.



FRENCH AND CASEMENT (CRANK TYPE) WINDOWS are difficult to secure. Slide or surface bolts can often be installed at the top and bottom of the window frame. Another method is to attach an "L" bracket to the lower portion of the window, as shown. Drill a hole into the window sill and insert a steel pin. The crank handle can also be removed for additional security.



SLIDING GLASS DOOR SECURITY. A commercial, key operated, locking device is recommended for sliding glass doors. The screws securing the locking device should be a minimum of 3 inches in length.



LOUVERED WINDOWS. It is best to replace these windows with another type. Metal grating may also be used as long as it is secured with large, one-way bolts, preventing the bars or grating from being torn free from their mount.

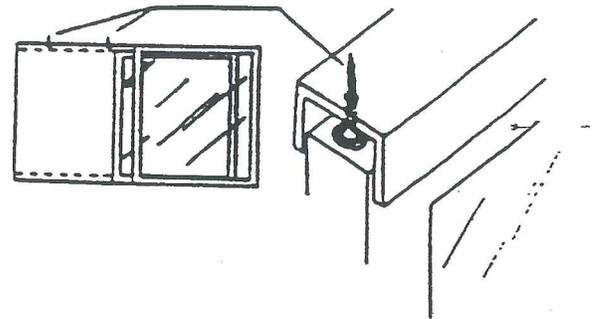
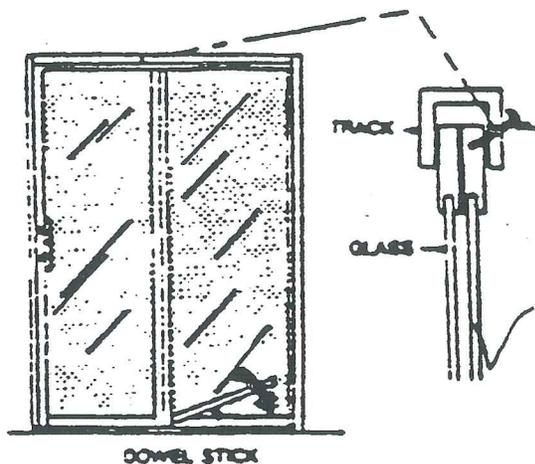
For the Interim period of waiting for the replacement window or installation of bars, you might want to secure the window as described below:

Individually remove each pane of glass and sand the glass and metal frame where the two meet.

Apply a two-part Epoxy Resin Glue to the sanded area. Replace the piece of glass into the framework and let glue dry.

ADDITIONAL TIPS ON SECURING SLIDING GLASS DOORS AND WINDOWS

DOWEL STICK OR STEEL PIN afford security to sliding glass doors. A simple way to secure an inside sliding door is to drill a downward sloping hole through the top portion of the sliding door frame. Insert a steel pin as illustrated. A dowel can be used to supplement.



ADDED SECURITY is provided by screwing two or three No. 8 or No. 10 sheet metal screws into the track above the sliding door. The screws should protrude so the top of the closing door just clears them. This will prevent the door from being lifted out of the lower track.