

PLAIN HISTORY GENEALOGY GROUP

Covering Plain, Sauk Co, Wisconsin and Beyond

<http://tinyurl.com/53dn2>.....*Haas Bauer Main WebSite*
<http://tinyurl.com/4t1rt>.....*PHHG ALL Newsletters & Meeting Handouts*
<http://tinyurl.com/4rrlv> <http://tinyurl.com/66w3v>..... *Newsletter Table of Contents*
<mailto:garylhaas2005@yahoo.com>.....*eMail Contact*
<http://groups.yahoo.com/group/phgg> *Yahoo! Group*
<http://garyhaas.blogspot.com>*Stuff I Find Interesting Blog*

Vol 25 Apr 2005

Change in eMail Address
Meetings & Events Schedule
Internet & Goodies
Hildegard Thering's Research Notes
Nifty Research Stuff
Protecting yourself on the Internet

E-Mail Address Change

I have a new eMail address. It is like the old address but with a 2005 in it.

DO NOT EVEN OPEN UP AN eMAIL FROM THE OLD ADDRESS garylhaas@yahoo.com.

Meeting & Events Schedule

Plain History Genealogy Group
Sat May 14th, 2005 9:30 am, Plain, WI
Kraemer Library and Community Center
2nd Annual Open House

This will be a great opportunity to find out what historical resources are available for family and local history research. You will also be able to discuss your individual research project with knowledgeable volunteers.

Some of the things we will have at the meeting for you to see, do and find out about:

- Watch 1930's movies of Plain
- Get help with Internet Research
- How to Scan Documents / Pictures
- How to use PDA's
- Wisconsin Historical Soc Library
- Sauk County Historical Museum
- LDS Church Resources
- St Luke's Chimes / Ox's Tail
- H. Thering's Research Notes

Come for the whole morning or just drop in to say hi. Things will be going on all morning. Hope to see you there.

For more information send an email to garylhaas2005@yahoo.com

Waldmuenchen Area Visitors
Plain, Wisconsin
Friday May 20th, 2005

Waldmuenchen, Cham, Bavaria, Germany is the ancestral home of many of the residents of Plain, WI. There will be a group of about 30 persons from Waldmuenchen visiting the Plain area on this weekend. The current plan includes a "town meeting" with these visitors in the Plain park area on Friday.

Milwaukee County Gene. Society, Inc. BIENNIAL WORKSHOP 2005

April 23, 2005

Serb Memorial Hall Milwaukee, WI

The featured speaker is Daniel M. Schlyter from the LDS Family History Library in Salt Lake City. I have been to his presentations before and they are very interesting and informative. He has a specialty in German Research.

Daniel Schlyter

- The Changing Map of Eastern Europe.
- Jan, Johann, John, Hans, Ivan, Juan, Jack.
- Understanding Germany and Its Records
- Using Vital Records to Build Your European Pedigree.

Bob Heck

- Internet Research Using the U.S. GenWeb - Part I
- Internet Research Using the U.S. GenWeb - Part II

Michael Edmonds

- Using Wis Hist Society Archives Digital Resources
- Using the Wis Hist Archives Collections in Madison

The presentations by B. Heck and M. Edmonds will be given at the same time as D. Schlyter's so you can only see four presentations.

<http://tinyurl.com/5c2ec>

German Workshop J. Humphrey Saturday July 9th, 2005.

UW-Whitewater Greenhill Center of the Arts

This is the annual genealogical workshop put on by the German Interest Group from Janesville, WI. I never miss this event. You can always learn something new.

- Developing the Skills to Become a German Genealogist
- Researching German Ancestors: the resources and the obstacles
- Exploring the German Character
- Finding Your German Ancestor's Place of Origin

<http://tinyurl.com/57kol>

Internet and Goodies

LDS Support by Email

<http://tinyurl.com/2cffy>

The people at the Family History Library of the LDS church in Salt Lake City is extremely supportive of ANYBODY's genealogical research. This website lets you send them your question in an email. This is a great tool for getting help.

Stories From Veterans

<http://www.loc.gov/vets/stories/>

I've always been fascinated by war and the people who fought in them. What makes a person willing to risk their life so I can safely watch cable TV in my apartment?

The Library of Congress launched a website dedicated to documenting "Experiencing War" on Memorial Day 2003. These are the digitized voices and words of the veterans describing their personal experiences. These stories a wide range of wars and battles from the view of the private to the view from the senior officer level.

PC Fagan Finder Google

<http://faganfinder.com/google.html>

The Google Internet Search Engine has lots of complicated "switches" that you can set. It can get very confusing. The Fagan Finder website gives you a nice "easy-to-use" form makes it easier to enter complex search queries.

German Life - Crime and Punishment

http://www.germanlife.com/Archives/1998/9812_01.html

This webpage has an interesting discussion of crime and Punishment in Early Modern Germany.

I has a special interest in this area because my gggg-grandfather was beheaded for killing my gggg-grandmother.

There was line of reasoning that justified torture:

- * a criminal was evil
- * needed encouragement to tell truth
- * torture was needed

Examples of some "normal" punishments

- * quartering or breaking on the wheel - aggravated murder
- * beheading - common murderers, robbers, forgers, arsonists

Dictionary of Wisconsin History

<http://www.wisconsinhistory.org/dictionary/>

Another great online tool from the Wisconsin Historical Society.

"Dictionary of Wisconsin History

These names of hundreds of people, places, things and events occur in many writings about Wisconsin history. Each is briefly defined here, and a source in which it is used or explained is cited. The Dictionary is being built chronologically and is currently strongest in terms from early Wisconsin history."

posted by gary h. @ 10:04 AM 0 comments

Steve Morse One-Step

<http://stevemorse.org>

There are lots of great sites on the Internet, but they can be laid out in a difficult to use format. Steve Morse's site gives you "easier-to-use" formats to access these great sites.

Morse covers the following items in "detail"

- Searching arrivals at Ellis Island
- Searching for information about ships
- Searching passenger records at Baltimore, Boston, Galveston, San Francisco
- Quickly finding census records
- Calendars, maps

Rootsweb Genealogy Research Guides

<http://www.rootsweb.com/~rwguide/#GENERAL>

The more you know about researching family and local history, the easier it gets. Rootswebs provide research guides that can help you learn the fine points of researching: ethnic groups and types of documents. This site is well-designed and easy to read.

New York Pub. Library Digital Gallery

<http://digitalgallery.nypl.org/nypl/digital/index.cfm>

NYPL provides free and open access to its Digital Gallery and images may be freely downloaded for personal, research and study purposes only.

They have hundreds of thousands of digital images that cover a wide variety of topics.

Here are some topics to search for:

- immigrants
- bremen
- wisconsin
- ships
- ellis island
- castle garden
- camp grant (WWI training camp)

Hunting Rabbits With Flash Lights

I have heard of hunting deer at night with flashlights. The concept is that you shine the light in the deer's eyes mesmerizing the deer into a paralyzed stop. Then the unsportsmanlike hunter shoots the deer. (This is where the phrase "frozen like a deer in the headlights" comes from.)

I was talking about old times with my dad the other night. He brought up about how they used to go shining for rabbits. This sounded nuts to me. Until he mentioned that they would go hunting rabbits at one or two o'clock in the morning. Hmm, isn't this about the time bars close down? I am sure that alcohol was involved somehow. My dad did not give me a specific time period when this took place. I am guessing the 1940s or 1950s.

He told us a story about how some guys shining rabbits shot up his trailer home one night.

He told us a story about how he, Delmar Ring, and Harry Diehl went out shining rabbits one night, They couldn't find any, so they went over to Eddie Weiss's farm where there was a brush

pile that was sure to contain rabbits. My Dad said that Harry Diehl had a big light that plugged into the cigarette lighter in the car. My dad has a vivid memory that when they shined into the brush pile, all he saw were the rabbit's ears. The shooting woke up Eddie Weiss who proceeded to yell at the young rascals.

As a personal comment, I wonder why I am not bothered about the ethics of hunting rabbits with flashlights. Could it be that rabbits are just a cute form of rats? Or that rabbits are tasty in a vinegar-based gravy?

Hildegarde Thering's Research Notes

Temperance Picnic htah0118.jpg

"On July 4, 1900, a temperance picnic was held at Plain in the Fred Schoenmann grove. At 2 p.m. Fr Vaughan of Eau Claire, who had a state reputation as an able orator gave the address. there was good music for the bowry dance. Lunches and other refreshments at all hours and amusements of all kinds furnished. A big dinner was served on the grounds."

Having a temperance picnic in a fun-loving German community must have been an easy sale.

Color of Busses htaa0095.jpg

"In 1939 the state legislature passed a law requiring all school bus owners to paint their vehicles red white and blue."

This was definitely different than the yellow busses i grew up. This must have created some vivid memories for the children riding the bus. This sounds like a great topic to research.

Nifty Research Stuff

WW II Army & Reserve Registration

You can access World War II Army enlistment records at the online NARA site (National

Archives & Records Administration.) This site has information on about 9 million enlistees.

You can find Clark Gable's enlistment record showing he started as a private in the Air Corps. The record shows that he had 2 years of high school.

Okay how do you find records? It is very tricky.

1. Go to http://aad.archives.gov/aad/file_unit_description.jsp?file_id=3475&coll_id=null
2. Click on the SEARCH button for *ENLISTMENT RECORDS Or RESERVE CORPS RECORDS*

Trick: Look for "Select from Code List" Instead of entering the State or County Name you need to enter a "Code".

Trick: Your Internet security settings might prevent the web page from loading. I can't get the link to work with my Mozilla Firefox browser.

Protecting Yourself on the Internet

The Internet is a great place to research. The Internet is as wild and uncontrolled as the Wild West, just like in the old days, a cowboy would not walk down the street without a six-gun for protection. You need to be packing some protection when you use the Internet. Today we are going to talk about how to protect yourself from some of the nastiness you'll run into on the Internet.

The bad news is that if somebody wants to get at your stuff, they can get it. What are the bad guys trying to do?

Some of the bad guys are trying to steal your personal information. Somewhere in your computer, you are likely to have your banking information, credit card numbers, passwords, Social Security Number and other stuff. The

bad guys use this information to get credit cards and run up large bills under your name.

Fortunately only a small percentage of identity theft cases involve computers. Most people's identities are stolen by friends and acquaintances, losing your billfold or purse, or people Dumpster diving in your garbage to get your bills and credit card statements. Some of these guys are trying to take control of the computer. A new trend is for the bad guys to try to get control of tens of thousands of PCs. These bad guys sell use of these machines to other bad guys to do nasty stuff.

If you use a dial up connection to get access to the Internet, some of these bad guys will change your local dial number to a number in Europe, so that you run up charge long-distance phone calls. Unfortunately, because of international laws, your local phone company cannot just reverse these charges. You're on the hook for them.

Some of these bad guys are just try to do damage to the information your computer, just because they can. There are lots of kids who think that it is cool to vandalized thousands of machines.

How are the bad guys doing it? The good news is that they rely on you to do something. They cannot get to your machine without your help. Generally, you have to click on something. The bad news is that you will click on something to give them access to your machine. No one is invulnerable, someday you will click on something you shouldn't because of a brain cramp.

E-mails are a common way hackers get at your machine. Just opening an e-mail with a virus from a hacker can cause problems. It is even worse if your e-mail automatically opens up attachments. Don't even respond to Spam that you get in your e-mail. Some e-mails have hidden attachments that tell hacker that they have a good address. Once a hacker knows that the good address, they will start to attack it.

Just visiting a web site can wreck your computer. Imagine that you went to visit a friend at their home, and as you were leaving your friend put something into your pocket. This is how these drive-by viruses get loaded. You visit the Internet site and it drops a nasty program onto your computer.

You have to be careful of pop-up boxes too. The really sneaky ones are so poorly worded that by clicking on no, you are really telling a hacker that yes, it's OK to do whatever they want to do with my machine. The safest thing to do is click on the X in the upper right hand corner of the window to close the popup box.

Remember there is no such thing as a free lunch. Cute toolbars that give you the weather, help you find files or help you share files are dangerous. If you use these "freebies" you have a good chance of having a virus loaded on your PC.

EULA stands for End User License Agreement. Most programs require that you agree to the EULA before you can use their program. Hidden in the incomprehensible language of these agreements, the bad guys have you sign your rights away to allow them to do whatever they want with your computer and information. Read these agreements carefully before you click on the button, agreeing to them.

Phishing is a new twist on an old way of getting at your information. The bad guys send you an e-mail pretending to be from your credit card company or bank asking to verify your information. Do not respond to these e-mails. A valid company would never ask you to re-verify your information through an e-mail or even a phone call. They typically would send you a letter.

There are Nigerian and genealogical e-mails trying to get at your money. The fraud is that they say if you send them a "few" dollars, they will send you thousands or millions. Getting involved with these e-mails has actually involved with some people being killed..

There are vigilante groups that are trying to combat these fraudulent e-mails. One vigilante group wrote back to the bad guys saying they would be happy to send the money, but it's locked up in CDs. This vigilante group said that if the bad guys would only send them a check to cover the withdrawal penalty, they would send the bad guys the money. One of the stupid bad guys actually sent a check to this vigilante group, which was promptly cashed.

Your children, grandchildren, and students can also let the bad guys get at your machine. They might think it's cool share music and programs over the Internet. To run a really cool game online, they might have to download a special program that has a virus in it. Letting people who are students use your computer can be dangerous, also. PCs at schools have a lot of different people using them. It is very easy to catch a virus at school and bring it to your home computer.

Microsoft has a very poor record for keeping your computer safe. Microsoft's e-mail programs Outlook, and Outlook Express, should be avoided at all costs. Microsoft's Web browser is another big problem. Even the Department of Homeland Security says that you should not use Microsoft's browser. Microsoft's Web browser allows sites to download stuff to your PC and take control of it.

Some of these things that are download are called browser helper objects or involve ActiveX. Some web sites use these things to do really neat things on their web pages. However, these really neat things can include viruses that will totally destroy the information on your computer.

Setting up a wireless network in your home can make it easy to share an Internet access. However if you don't set up the wireless network properly, anybody and their brother can get access to your stuff. The default settings for wireless networks are well known by hackers, and they will use them to get at your stuff. Some hackers even drive around with laptops in neighborhoods to see who has unsecured

wireless networks. They then share this information with the "world" over the Internet.

Instant messaging, chat rooms, and online games can be fun. From personal experience, they can also make you a target for hackers.

OK, how do you protect yourself? Your approach to protecting yourself should be that you accept that your PC WILL BE HACKED. There are things that you can do to make it difficult for the hacker. But you have to be prepared when your PC is attacked.

After badmouthing Microsoft's poor security, I was kind of surprised that Microsoft has excellent videos on a protecting yourself on these web sites.

<http://www.microsoft.com/athome/security/default.mspx>
<http://www.microsoft.com/athome/security/protect/default.mspx>

The first thing you can do to protect yourself is to be careful what you click on. Don't click on e-mail attachments. Don't even open up e-mails from people you don't recognize. Don't just quickly click on a pop-up box to get rid of it. Unfortunately, no matter how careful you are, you eventually will click on the wrong stuff.

Another thing you can do is to keep your personal information safe. Don't put your bank account number, credit card number, Social Security Number, or other personal information on the Internet, unless you are 100% certain that you were dealing with a good site. It's important to keep your personal information secret. Keep your personal information recorded in just a few, safeguarded secret places.

Another way to protect yourself is to use throwaway IDs when you are working with Internet sites. Only share your primary ID with people and sites that you trust.

To protect yourself, you need to know when your PC is acting funky. Like a doctor, you have to watch your PC for symptoms that it has been hacked. It is important to know what is normal for your PC. This includes things like:

- How long does it take your PC to startup?
- Is your PC running slower?
- Does your PC crash more often?
- Has your Internet home page been changed?
- Do you have new toolbars on your Internet browser?
- Are you seeing more pop-up ads?

Knowing what is normal for your PC makes it easier to identify when you have a problem.

Make a list of your subscriptions, login codes, key program codes, your credit cards and other financial information. Be prepared when somebody attacks your machine. They could be trying to steal your identity. The quicker you can close accounts and change passwords, the safer, you will be. Having a list makes it easier.

An easy way to protect yourself is to use strong passwords. Use at least six characters including letters, numbers and symbols. I personally don't mess around with using upper or lowercase letters. If your password is so complicated that you have to write it down, this can make it easy for hacker to find your password on a note stuck to the side of your computer.

One way to create a safe password that is easy to remember is to start with a phrase that you can easily remember. For example, The Quick Brown Fox Jumped over the Lazy Log, is an easy to remember phrase. Use the first letters of each word as a password. Change some of letters to a number that looks like a letter. For example, use the number one for the letter l, the number zero for an o, the number five for a s. This gives you the code **tqbfj0t11**. (Don't use this phrase. The hackers know to check for it.)

Changing the security levels and defaults on your PC can make you safer. There are lots of stuff on your computer that you don't need.

If your computer is set up to share files, turn the sharing off. Having file sharing turned on can be dangerous, especially if you're using a cable modem Internet connection. "Everybody" can share your files as though they were sitting at your computer in your home.

Disabling the Microsoft messenger program is even recommend my Microsoft itself. This is a feature that is usually only needed by big businesses. (This is not the instant messenger program from Microsoft.)

Disable any programs that you don't really need. How do you know if you don't need a program? There are sites like the Black Viper, which can help you figure out which are the programs to turn off.

<http://www.blackviper.com/WinXP/servicecfg.htm>.

Lots of the programs that make a web site look spiffy, also allow hackers to get at your machine. In your browser program should turn off or disable the options related to: ACTIVE X, JAVA and SCRIPTING.

There is a spot in the browser's option page to set the security level for your PC's browser. It can be tricky to find, but it will make your PC safer.

Some people have fits over the cookies that some web sites use the track information about you. If you use the recommendations in this article, cookies should be OK.

You might want to switch to a new browser that is less prone to hacker attacks. Firefox is a great alternative browser.

As with most things that are computer-related, changing things and disabling options can break your computer. There are a number of web sites that will not load properly, if you change your security settings.

Lots of hackers try to attack your machine through your e-mail. Online e-mail accounts can be safer to use because they typically have built-in virus scanning, and you typically have to click on an attachment to open it. I use the online e-mail provider Yahoo!. The cost is \$20 a year to get extra security benefits and a whole lot more storage space. Yahoo! also lets you set up numerous addresses for the same e-mail account. I use these throwaway e-mail addresses when I respond the something on the

Internet. If a hacker gets a hold of this throw away e-mail address, I can just turn it off. Plus using these throw away e-mail addresses let me see where the problem e-mails are originating from.

There are three programs that every PC needs to have installed; firewall protection, antivirus protection, and spyware protection. You should check the status bar at the bottom right of your PC desktop window, where you should find an icon for each of these programs. Make sure that the icons are active.

When you attach your computer to the Internet, it is like you are left all the doors and windows to your house wide open and put a big neon sign outside saying, "Please Come in, Get My Stuff." Firewalls close all the doors and windows to your PC to keep the bad guys out. Firewalls come in a hardware format called routers. I use the software version firewalls because it is easy to install. I pay \$40 a year for the commercial version of Zone Alarm. There is a free version of Zone Alarm that will do the job for you also.

In the nine months since I last installed Zone Alarm, it blocked over 95,000 attempts to ask is my machine by over 100 different hackers. They have done studies in it only takes about five to 10 minutes for hacker to locate a PC without firewall protection.

When you first install Zone Alarm, it totally prevents all programs from accessing the Internet. You have to specifically tell Zone Alarm which programs are OK to access the Internet. This is the only way that you can be sure that a hacker's program doesn't have access to your PC. There are three different ways that Zone Alarm controls access to the Internet. It can DENY access. It can ALLOW access. It can PROMPT you every time the program tries to run. For programs that you want to run all the time, like your Internet browser, you can tell Zone Alarm to "remember" your response. This allows the "approved" program to "automatically" access the Internet. You can use this to permanently turnoff "nasty" programs' ability to access the Internet.

<http://www.zonealarm.com/>

You need to have an antivirus program running at your PC at all times. I use Norton antivirus, which is part of their System Works program. AVG is a free antivirus program will also do the job for you. Most antivirus programs will give you give the option to automatically update themselves for new viruses,
http://www.grisoft.com/us/us_index.php.

You also need to check for and remove spyware from your PC on a regular basis. No matter how careful you are, spyware will find its way onto your computer. There are lots of programs that say they can do the job. BE CAREFUL. Some of the programs that say they will get rid of the spyware from your PC will actually load their own version of spyware onto your computer.

If you are using Microsoft XP, I strongly recommend that use Microsoft's Anti-Spyware program. Based on tests by independent people, this program will catch more spyware than any other program. It will also detect and remove spyware that it finds. It will also stop spyware programs from installing themselves in the first place, keeping them from becoming problems. The program automatically updates itself. I have the program set up to scan my computer, every day at three o'clock in the morning. IF YOU ARE A GEEK, MICROSOFT'S ANTI-SPYWARE PROGRAM HAS TREMENDOUS DIAGNOSTIC REPORTING THAT WILL TELL YOU LOTS OF THINGS ABOUT WHAT'S LOADED ON YOUR PC.
<http://tinyurl.com/47cus>

If you don't have Microsoft XP, you can try the programs made by Ad-Aware and Spy Bot Search and Destroy. All these spyware programs are free.
<http://www.lavasoftusa.com/>
<http://www.safer-networking.org/en/index.html>

Watch out for the bad guys when selecting an antivirus/spyware program. They sometimes use a name that is similar to a valid antivirus/spyware program hoping you will load

their "nasty" program, which will then load its own flavor of spyware.

Because hackers are developing and releasing new viruses and spyware programs daily, you'll need to keep your protection updated. I have my firewall, antivirus, and my spyware program setup to update themselves daily. I also update my Microsoft's operating system on a regular basis.

Even if you do all the right things, some things will sneak through and load themselves onto your computer. I trust my protection programs to keep me safe, but I like to verify that nothing has snuck onto my computer.

There are 2 great Internet sites that will run checks on your PC, looking for bad stuff or weakness:

- Gibson Research Shields UP
<http://grc.com/default.htm>
- PC Pitstop www.pcpitstop.com

Every now and then I like to check to see if any my personal information has made it out to the Internet. I use the Google Internet search engine to check my name, address, and key identification numbers. With identification numbers, I will use the number range search feature of Google. I never typed the actual ID number into Google.

Your PCs has been hacked, now what you do? The first thing you should do is to find yourself a geek. Some of the programs to hackers use are so difficult to remove you need an expert.

You might want to disconnect your PC from the Internet. Some of the nasty programs will reconnect to the Internet, to prevent you from cleaning them out.

Back up your data. Removing a spyware or virus program can be messy. It is possible that you can totally hose up your machine to the point that you have to reformat the hard disk and start over.

Before you can cleanup of virus or spyware program, you have to know what's running on

your machine. You can use the three-finger salute (CTRL ALT DELTE) on your PC to bring up the task manager. This will give you the cryptic names of what is running. But even a geek has trouble trying to figure out which are the good programs in which are the bad programs.

Hijack This is a great program for finding out what's on your PC. It gives you a listing of what is running on your PC, which can be posted to a number of Internet web sites were geeks can analyze it and give you recommendations on how to fix your machine. Only a geek can understand the listing.

<http://www.merijn.org/index.html>

Belarc Advisor gives you a more complete and easy-to-read listing of what's on your machine. It gives you a list of software and hardware install on your machine. The list includes all of the Microsoft patches that have been installed. The list also includes the security codes needed to install software. There is an extremely detailed and lengthy list of all the software loaded on your PC, including the version number. You can e-mail this list to your geek friend, so they can diagnose the problem. YOU SHOULD RUN BELARC ADVISOR JUST TO GET A PRINTED LISTING OF WHAT IS ON YOUR PC.

http://www.belarc.com/free_download.html

Microsoft AntiSpyware does the best job of explaining what is running on your PC to. It gives you fairly clear description of what the program does. It will also tell you if the program is known to be safe, be dangerous or is unknown. <http://tinyurl.com/47cus>

There is a great web site that has short, easy to understand videos on how to use some of these tools. www.savemybutt.com/video.php

Online How-To Videos

- Ad-Aware
- Spybot Search & Destroy
- Steve Gibson's Shields Up
- Using Belarc Advisor

Once you have identified the virus or spyware program, the next step can be tricky, removing

it. Most of the protection programs that I have recommended automatically will remove the virus or spyware program.

If they don't, you can check out the program on Google and Google Groups. Search for the program's name or the error message that the program causes. There are lots of helpful geeks that will tell you how to fix your PC, usually in understandable language.

Spyware Warrior is a tremendous web site that has a place where you can post your Hijack This listing. <http://spywarewarrior.com>

You have to be prepared for the worst possible scenario, which is to reformat your hard disk and reinstall your software. This is one reason you should make regular backups.

My Yahoo! e-mail account was just recently hijacked. It was my fault, I had an extremely weak password that was easy to crack. And I forgot the answer to the SECRET QUESTION that I answered seven years ago when I first set up the account. Pleading to Yahoo! didn't do any good. My e-mail account was locked up and there was no way I was going to get access to it again.

I believe my account was hacked by somebody I played Pinochle with on Yahoo! There are lots of idiots out there that don't like to lose. The lesson, I learned here was to have to separate Yahoo! accounts: one for my e-mail and one for the games.

Now, I also subscribe to a service that automatically monitors my credit ratings and notifies me of any changes by e-mail. The service costs \$12 a month. I consider this cheap insurance against somebody stealing my identity.

What are the security measures used to prevent any Joe Schmoe from accessing your detailed credit information online? I subscribed to this service over the Internet without having to talk to a person. The online service "verifies" that you are the right person by asking you a

question about an account on your credit report. If somebody had Dumpster dived in my garbage, they could have easily answered the question and gotten access to my information.

This is why I use a shredder for all my sensitive papers. This prevents somebody from going to my garbage to find out information that would be helpful to stealing my identity

Another thing you can do is to call the three national credit-reporting organizations and place a "FRAUD ALERT" on your name and social security number. Any company that checks your credit report will "know" that they should contact you before extending credit.

- Equifax 1-800-525-6285
- Experian (formerly TRW) 1-888-397-3742
- Trans Union 1-800-680-7289

SUMMARY.

- Be prepared for WHEN, not IF you are hacked.
- Think twice before clicking on something.
 - E-mails from unknown centers.
 - Attachments (even if from "friends")
 - End User License Agreements
- Think "4 times" before sharing personal data.
- Watch out for bad guys, pretending to be your friend.
- Know what is normal for your PC.
- Document what you have on your PC.
- Use strong passwords.
- Use firewalls, antivirus, spyware program.
- KEEP THINGS UPDATED

One final negative thought, no matter how hard you try, your stuff is at danger. Major companies like ChoicePoint and Bank America have recently "lost" or "released" key customer data. This information is not floating through the Internet. And the nasty thing is these bozos wouldn't tell you if they "lost" your information if they had a choice. Fortunately California requires that companies notify their customers when their personal data has been placed at risk.