Identity Theft; The Other You Has Stolen Your Identity ~ How to Stop Him/Her!

"Preventative Measures You Can

Take to Reduce the Chance of Identity Theft from Happening to You"...

by Terry Clark

Table of Content

8. Prompt Actions Against Identity Thieves

9. Losing your identity over the internet

10. Insurance for identity theft victims

11. Dealing with Inevitable Website Scams

12. Can You Stop Credit Card Identity Theft?

13. Beyond Identity Theft Law

14. Avoid Identify Theft from Obituaries

15. The Identity Theft Quiz

16. How To Prevent Identity Theft By Computer Hackers

17. Identity Theft is Still at Large

18. Tax Season is Bringing Out Identity Thieves

19. Identity Theft And The ATM Game

20. Identity Theft: Up In A Down Economy

21. Think You Don't Need a Shredder? Think Again

22. The Young Victims of Identity Theft

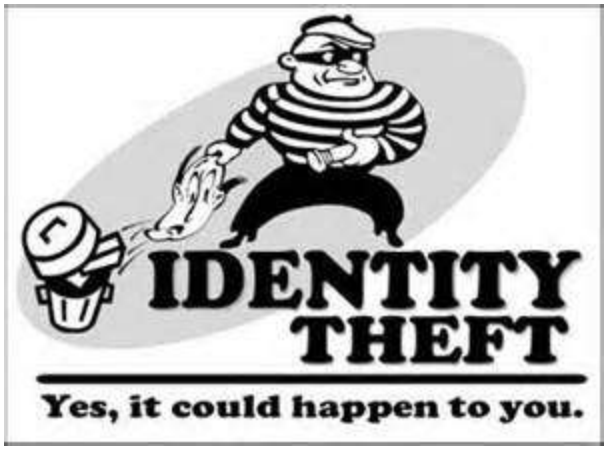
23. Identity theft and fraud criminals are turning their attention to senior citizens

24. What is Business or Commercial Identity Theft?

25. Can Vacationers And Business Travelers Be At Greater Risk Of Identity Theft When They Travel?

26. Will Obamacare Lead to Identity Theft?

(Recommended) Resources to Protect Your Identity.



#1. What is Identity Theft?

Identity theft is a crime. Identity theft is a term used to refer to all types of crime in which someone illegally obtains and uses another person's personal data in a way that involves lies or deception, mostly for economic gain.

Identity thefts is one of the fastest growing crimes in the country and what can be really frustrating about this is that you cannot really know how fast it is growing. Not only are identity theft cases hard to solve, they are also hard to detect. There are identity crimes that are not solved until after a decade because of the lack of information. Remember that though these crimes may be easily detected through credit card purchases, there are some con artists that do not use that avenue. What they do is just assume your name and personal history and use it as their own.

Unlike your fingerprints, which is impossible to copy, your personal data especially your Social Security number, your bank account or credit card number, your telephone number, and other identifyable data can be used, if they fall into the wrong hands.

In the United States and Canada, for example, many people have reported that unauthorized persons have taken funds out of their bank or financial accounts and in the worst cases, took over their identities,

obtaining huge debts and committing crimes while using the victims's names. In these cases, the victim's losses may include not only financial losses, but additional financial costs associated with trying to restore his reputation.

In recent years, the Internet has become the perfect place for criminals to obtain personal data, such as passwords or even banking information. In their haste to explore the exciting features of the Internet, many people respond to "spam" unsolicited E-mail that promises them some benefit but requests identifying data, without realizing that in many cases, the requester has no intention of keeping his promise. In some cases, criminals reportedly have used computer technology to obtain large amounts of personal data.

If you have received mailed in applications for "preapproved" credit cards, but have thrown them in the garbage can without tearing up the enclosed materials, criminals may retrieve them from the trash and activate them without your knowledge. (Some credit card companies, when sending credit cards, have adopted security measures that allow a card recipient to activate the card only from his or her home telephone number but this is not yet a universal practice.) Also, if your mail is delivered to a place where others have ready access to it, criminals can just intercept and redirect your mail to another location so that they will receive them.

With enough identifying information, a criminal can assume an individual's identity and conduct a wide range of crimes: for example, applications for loans and credit cards, withdrawals from bank accounts, use of telephone calling cards, or obtaining other goods or privileges which the criminal might be denied if he were to use his real name.

If the criminal takes steps to ensure that bills for the falsely obtained credit cards, or bank statements showing the unauthorized withdrawals, are sent to an address other than the victim's, the victim may not even be aware of what is happening until it is much too late when the criminal has done much damage to the victim's assets, credit, and reputation.

#2. Tips to Prevent Identity Theft

The time it takes for a victim to recover from identity theft can be extensive, and while the wounds aren't physical, they are psychological and life-changing in several ways.

Identity theft occurs when someone steals personal information and pretends to be you to obtain credit cards, loans, and even jobs by using your work references.

Identity thieves only need to know your Social Security number, name, and address to wreck your good credit. Using easily accessible public records, they can learn your place of employment, date of birth, and mother's maiden name. They can open a credit card account and immediately charge up to the limit with no intention of paying.

Credit cards can be obtained through banks and credit unions as well as chain stores. Many offers for "pre-approved" credit cards come in the mail.

Getting a credit card issued by department stores is simple. Only two forms of ID are required: a driver's license with a picture ID and a second identification, like another credit card or your Social Security card.

What steps should you take to protect your identity with credit cards?

Ask stores at which you are applying for credit how they safeguard credit applications. Ensure that they are treated as secure documents.

Ask businesses how they store and dispose of credit card transaction skips. Ensure that proper safeguards are in place to treat these documents securely.

Never giver credit card numbers or other personal information over the phone unless you initiate the call. Even if you initiate the call, ensure that called party is not using a cellular or other mobile phone.

Carry only the credit cards needed for the current trip. Most people carry all their credit cards with them at all times.

The garbage bags are not secure place for old or pre-approved cards. Tear them up before throwing them away. Thieves can retrieve these documents and open credit accounts with new addresses.

Keep a list or photocopy of all credit accounts, along with expiration dates and phone numbers to call in case of theft. Keep this list in a secure spot at home.

When you purchase items with credit, always take your credit card receipts with you. Never toss them in a waste basket.

Do not have boxes of new checks delivered to your home. Arrange to pick them up at the bank or credit union.

(Do not write credit card numbers on checks).

If you have applied for a new credit card and it does not arrive, contact the issuer.

Avoid giving credit card numbers over the phone if you are in a public place. Even at work, others may overhear and use the information.

#3. Safeguarding Your Social Security Nunber

High tech communications have raised notoriety in the rampant theft of identification numbers. The mightiest business tycoon down to the lowest ranking employee in a corporation, company, or any enterprise owns a kind of identity number attached to his being member to any social security group, or kind of financial management for use in billings, daily expenditures, and savings. It maybe, identification number on social security, insurance, banks, or anything that could be a means to access individual cash settings, or safekeeping. Identity number is enough to allow a loan process, cash credits, or deposits.

Other identity numbers, such as specialized ATM's, Credit Cards, Master Cards, issued for high end use, and benefits with high potential credibility, are approved and released on strict and stiff screening process that allow the individual, to use on

international travel and expense abroad, instead of carrying cash bulk, or money transfers that entail more time and effort. Using any credit account or savings deposit card in today's modern-day purchasing is most convenient and safe.

How to Evade Being a Victim to Identity Number Social Theft

• Never disclose your personal address and telephone directory that easy to anybody, unless you fully trust a person, or, he's proven to have displayed the best of character, habits, and attitude for a number of years in your lengthy work, and friendly experiences together.

• If you are using see-thru plastic envelopes for documents in process, try to shield them from direct curiosity of anyone. Exposed content identity number on way to documentation and office tours could be stolen instantly by a mere peep. People are trained so effectively for certain specific purposes, right or wrong. Remember, individuals have personalized objectives to work out with, on various angles they're trapped into. And, possibly, one of those identity number social thefts may be tagging along target workplace areas for their misdemeanors.

• Be vigilant about consistent updates on Credit Annual Reports Thru it, you'll know if there had

been a change in the gap and frequency of transactions on loans and utility billings, and its outstanding balances. Take a note if there are irregularity listings on address and other basic data.

• Don't answer directly from your landline telephone, nor you'd reply straight to the caller in his telephone or mobile unit for any demand on your personal identity number, or number. Queries needing response that you find doubtful should be replied direct to the office referred to, in the call. Possibly, try to research about the whereabouts of the place mentioned, if there are any.

• Provide password to your network accounts to avoid general access in the https site that could be notably encrypted by general computer users. Never give personal information tips to any website if they are not locked with SSL (Security Socket Layer).

There are many reasons why Identity Numbers Social Theft does exist. Others start from habits to deviate from the usual norm of conduct, and insist on doing things negative. Some wants it the easy way to earn, but risks are, to their disadvantage. It takes years to redeem looses if we fall victim to it. Having attained full control in the "hide and seek" from the law games, it is futile to get immediate solutions.

We owe it to ourselves to be on guard against anyone seemingly of doubtful character.

#4. Robbing someones Credibility

Identity theft in a broad sense covers many categories in courtroom battles. When identity theft is set for trial, this is no ordinary stealing of one's number, or mere misrepresentation of some data common to salespeople, neither for the reason of lying, commonly mistaken as fraud for easier grounds to legal access.

Rather, it is the criminal deeds about the theft done by deception behind that stealing, misrepresentations, or lying. Identity theft and fraud is perfect combination to create a sophisticated crime in the immigration, espionage, frame up a crime, access to somebody else's finances for economic gains. Identity theft and fraud is worst than plain robbing of any material goods, or common personal belongings.

Notorious criminals gaining control over important data of checking accounts, credit cards, social security, telephone numbers, passwords to either website or bank accounts, certainly will create havoc. Aside from using influence over one's name

thru purported deceptions, he will continue committing bad actions under one's name to destroy long-established good reputation. Identity theft and fraud is one bundle of gigantic crime package that could start with a solicitous demand of one's social security, or telephone number.

From there on, a criminal goes on manipulating to get further data from the victim's trusted relatives and immediate family. Hands-on criminals never cease at one victim, unless they devour them, whole into his system. Once access is gained, will continue to finish with him rather than get started with another.

Common Ways to Evade Being a Victim of Identity Fraud:

1. It's a rare case that someone will ask you about your middle initial (mother's surname), if it happens, never divulge it. Obviously, banks or other financial management companies have already put them on records, and another attempt to get thru the like data is certainly created by somebody else's, other than where your inputs are.

2. Be careful not to throw away your returned checks on paid billings from your paying banks. There might be scavengers loitering around for the purpose of following up garbage to get checking account numbers, and other data.

3. Originally approved Credit Cards, or renewals of the same, may be delivered by servicemen who may try to get your personal data that are not commonly asked, such as birthdays, or expiry dates of your card. Refrain from it, instead, tell them to send you a written message, bearing the letterhead of the originating office that they need it, to add to your resume.

4. Never endorse any possible letter in your mailbox, if you go on vacation unless to a trusted friend or relative. Your letter bearing your address might not get into your hands at all, bits of essential information, leaked instead.

5. Always be aware if you're on call at a public telephone, somebody else may over hear you if you are transmitting some confidential matters concerning your personal identity.

Of course, no matter how careful, or effectively oriented a person may be, at times things just happen inevitably, or without much awareness. A possible victim of identity theft and fraud has only these offices to go in order to minimize further damage to his finances, reputation and disadvantage to his economy.

- **Contact by all means the FTC (Federal Trade**

Commission), and report the case immediately.

#5. Reporting Identity Theft

If you are a victim of identity theft you are not alone. You are just one of those nameless individuals struggling to reclaim their identity. Countless people have been victimized by this crime and have lost everything. So if you are a victim tell other people and tell it to the right people.

Report identity theft:

If you have been a victim, do not hesitate to call the police or any authorities that can help you. Remember that this is not just a simple theft that you can just forget about afterwards. Losing your identity can have a lot of repercussions not only in terms of personal properties but also with social reputation. And because identity thieves are real slick, authorities would not know what is happening unless you tell them so. They would not even know that there are "two" you without you saying that there is. Only by making an effort to seek the proper authorities and report your case will you be able to help fight this growing criminal bandwagon.

Report identity theft to the police:

To report identity theft, you will need to visit your local police station. Many people find this experience intimidating. They may also worry that the police will try to hand the guilt over to them or make them feel stupid for being victimized in the first place. But this is not the case. The police in your area will probably have experience dealing with these types of crimes and will understand your feelings. Just remember their job is not to make you feel better, but to help you catch the criminal.

When you report identity theft to the authorities, take with you some evidence such as your credit report, statements from any accounts opened in your name without your authorization, and/or any other documentation that the crime has taken place. You'll also need to bring a list of all the accounts that have been affected by this crime, so the officer can include that list with your report.

Report identity theft to your creditors:

After you finish filing the report, you'll want to make many copies of your police report. Every creditor and financial institution with whom you do business should receive a copy of that report along with a letter explaining that you have been the victim of identity theft. Make sure that you hold onto the original police report because you may need to make even more copies. Copies should also be sent

to all three credit reporting agencies.

Report identity theft to the FTC:

Even though the police station would be the first people you will think of when asking for help or when reporting an identity theft, do not place much hope that the police will get very far in investigating your case. Identity theft cases rarely end in arrests because the guilty party can too easily cover his or her tracks. However, after you report identity theft to the police, you should contact the Federal Trade Commission (FTC). The FTC is the government agency through which all the cases of identity thefts must pass through before being investigated at the federal level.

The FTC Website:

http://www.ftc.gov/bcp/edu/microsites/idtheft/ to file your complaint and for additional steps to take if you've been victimized by identity theft. The FTC may not be able to help you regain what was lost when your identity was stolen but their far-reaching investigations and statistics analysis can be helped if you report identity theft.

#6. Questions From an Identity Theft Victim

Identity theft is a crime in which the imposter obtains key pieces of information such as Social Security and driver's license numbers to obtain credit, merchandise and services in the name of the victim.

The victim is left with a ruined credit history and the time-consuming and complicated task of regaining financial health. The imposter may even use the victim's good name for criminal activities. It is a dual crime because not only is it committed against an individual's financial life and credit history but also against his or her reputation and social standing in the community and in the workplace.

In one notorious case of identity theft, a convicted felon have not only incurred thousands of credit card debt by using another person's identity, he was also able to obtain a federal home loan, and even bought homes, motorcycles, and handguns using the victim's name. What is even more frustrating is that the felon even called his victim to taunt him -- saying that he could continue to assume the victim's identity for as long as he wanted because identity theft was not a federal crime at that time. After which, the felon even filed for bankruptcy, also in the victim's name.

While the victim and his wife spent more than four years and more than $15,000 of their own money to restore their credit and reputation, the criminal

served a brief sentence for making a false statement to procure a firearm, but made no restitution to his victim for any of the harm he had caused.

How do thieves get my information?

• They go through your trashcan, looking for straight cut or unshredded papers.

• They steal your mail or your wallet.

• They listen in on conversations you have in public.

• They trick you into giving them the information over the telephone or by email.

• They buy the information either on the Internet or from someone who might have stolen it.

• They steal it from a loan or credit application form you filled out or from files at a hospital, bank, school or business that you deal with. They may have obtained it from dumpsters outside of such companies.

• They get it from your computer, especially those without firewalls.

• They may be a friend or relative or someone who works for you who has access to your information

Tips to Consumers:

How can I prevent identity theft? While no one can totally prevent this crime from occurring, here are some tips that can help you decrease your risk.

• Check your credit reports once a year from all three of the credit reporting agencies listed below.

• Guard your Social Security number. When possible, don't carry your Social Security card with you.

• Don't put your SSN or drivers license number on your checks.

• Guard your personal information. You should never give your Social Security number to anyone unless they have a good reason for needing it.

• Watch for people who may try to eavesdrop and

overhear the information you give out orally.

• Carefully destroy the documents that you throw out, especially those with sensitive or identifying information. A crosscut paper shredder works best.

• Be suspicious of telephone solicitors that call you at your office. Never provide information unless you have initiated the call.

• Delete and do not reply to any suspicious email requests.

• Use a locked mailbox at your home to send and receive all mails.

• Make an effort to reduce the number of preapproved credit card offers that you receive.

Protecting Identity is More Than Protecting Individuality

Do you remember that Hollywood blockbuster several years ago involving a woman that needed to keep running because of a compromised identity with information taken from the Internet? Or more

recently, there was yet another Hollywood offering that shows a regular family man's ideal home and family turned into a suspense-filled arena for a bank heist because of sensitive information gathered from the family trash?

Although, as the disclaimer at the end of these films say, these stories are fictitious, there is indeed cause for alarm for things like these happening to you. Identity theft is a growing problem and once you've been victimized, a whole slew of difficulties will arise from this crisis.

Don't panic just yet though. Note that from these movies you will see that these types of identity thefts are done with precision and motive. Meaning, when identity theft to that magnitude happens, it is usually committed by someone who knows your personal habits and may not be a serial identity theft. That means, you need to safe guard against friends or family that may have a drug problem or are in dire financial straits. Suspicious of you to think this way sure but as the cliché goes, it is better to be safe than sorry, and believe me, sorry is the least of your worries if you become the hapless victim of identity theft.

Just think-if your wallet was stolen or you have for one reason or another, been physically separated from items that contain sensitive information like your social security number, credit card information, driver's license number, etc-- it is

easy to prevent identity theft because you can cancel all your cards and report them stolen to prevent anyone misusing your personal information for their gain.

Now imagine this-you are hounded by credit collectors for purchases you have not made, or worse-you are wrongfully apprehended for a crime you most certainly did not commit. How did this happen? Your personal information and sensitive numbers were never physically separated from you. Unfortunately, carelessly giving away your social security number or other sensitive information may put you at risk for identity theft.

A database with all your information may be sold to another entity that may use your data to make purchases in your stead without you knowing. It's easy enough if the criminals who commit identity theft will make purchases on your existing credit cards and such. You can easily check your existing credit cards and see fraudulent purchases.

What about checking the accounts that you don't know about?

Identity thefts may open new accounts for mobile phones, credit cards and even make larger purchases like buying an apartment and you won't know it unless the credit collectors finally trace the bills back to you after the perpetrators run off with the bills.

Therefore, identity theft protection is important, as you have now surmised. Although as in everything in life (another cliché coming), prevention is the best cure. Given this, it is important to find out the best ways to prevent and protect yourself against identity theft. Fortunately, you can get extremely useful information on this online through websites like www.crimedoctor.com

This website is a rich resource for anything and everything about identity theft and how to protect yourself against it. This site has a very useful article on identity theft written for lay people like you and me so that you can guard yourself by learning more.

#8. Prompt Actions Against Identity Thieves

Identity Theft soars high in crime reports at the U.S. Federal Trade Commission (FTI) and other government bureaucracies; credit report agencies, Forensic Accounting firms, investigators, and other private consortiums to protect victims. Any holder of information identifiers of social security number, credit cards, bank account number, driver's license, health care, and other financial sources is at risk. Everyone is vulnerable, offline or online. Households, telephone booths, and garbage areas are common places where criminals

loiter around to look for their prey. Thieves simply want it the easiest way to earn without exerting much effort.

If a culprit gets into hands-on control of one's number, it could be a start of a cycle of indefinite crimes against the legitimate owner, would lead the poor victim and his family into rubbles of chaos that can't easily be repaired. A ruined reputation because of unprecedented debts thru malicious intent of someone would ruin anyone's credibility, and totally, his life. There's no way patching it up immediately, for criminals have all pretext to blackmail his victims pestering him further to the police.

If you're a victim of identity theft, never loose time to research primarily in troubleshooting your problem. It is not easy, for the authorities at times will not listen. Going to agencies to get solutions entails a lot of expense. A victim will be entangled into questions of how, what, who, and where to get thru your complaint, or report. Get proper forms of applications of your complaint at the proper government agency.

Once filed, if its with the FTI, being the leading and core authority to follow-up of credit records trespassing, it has full control to *detect, by way of consistent monitoring of your financial accounts as well as your current billings; *to deter, with caution to safeguard any personal information data

under their safekeeping; *defend your identification from any continuous manipulations of the suspected theft.

Having lost your credit account to the hands of a thief, you'll need to hire a Certified Forensic Accountants (CrFA's), who investigate to the in-depth of the irregularities of your figures in record that affect your monetary condition badly. It composed of CPA's, CrFA's, and investigators who will help you in all angles of your financial loss to the offender. Most importantly, it will handle the defenses against any repetition of identity deception.

Generally, federal prosecutors cooperate with various investigating agencies to prosecute any identity theft fraud. These are the FBI, The U.S. Secret Service, and the U.S. Postal Inspection Service.

A lot of paperwork is involved when you are filing your complaint to a definite jurisdiction of theft offense. You'll need a series of contact files, actual conversations and written messages, discussions at the agency, dates, and witnesses, if there are any. Original copies of all documentations should be included in your files.

Send out to any office or person concerned photocopies only. A summary of what happened

should be included in the report. The process is very meticulous and needs ample patience and determination. Ready your self for years of waiting before the offender will be found and proven guilty.

It would be too hard to mend a lost spirit on your part for having lost some of your economic gains that can't be recovered in years, alongside a weakened morale. Be serious in shielding yourself against identity thieves before becoming their prey.

#9. Losing your identity over the internet

Having someone steal your identity seem to be the stuff that science fiction books and movies have on their convoluted plots. But that was before… before the rise of technological advancement, before the creation of the world wide web.

Now, identity theft is no longer a dream for some hackers and internet con artists. One can even say that with their techniques and expertise, it will be like taking candy from a baby… yet this time, it involves more than sweets. Life is at stake, personal and social life.

How can someone steal your identity? By asuming your

name, Social Security number, credit card number, or some other piece of your personal information for their own use. In short, identity theft occurs when someone uses your personal information without your knowledge to commit fraud or theft.

They open a new credit card account, using your name, date of birth, and Social Security number. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report. They call your credit card issuer and, pretending to be you, change the mailing address on your credit card account.

Then, your imposter incur charges on your account in your name and have the bills sent to the new address. This is why most people may not immediately realize that there's a problem. They establish cellular phone service in your name.They open a bank account in your name and write bad checks on that account.

How Easy is it to Get Personal Information?

The amount of information available on the Internet about you and those you know is almost unbelievable. Various companies offer services that provide address, criminal, civil, and professional history as well as a list of assets and bank account numbers. Also available are the Social Security number, last six addresses, current phone number as well as names

and phone numbers of neighbors. Some large, prestigious companies offering such information include Lexis-Nexis and West Publishing Company.

Many smaller companies also provide similar services.

This research used to take days. Today, this information is available in minutes with only a few click of your mouse. Here are economical products that can help uncover personal details you thought were strictly private.

Identity theft involves someone using key pieces of your identifying information in order to impersonate you. The usual purpose is to acquire goods or services in your name through the use of credit or debit cards. The U.S. Postal Service calls it the "one of the fastest growing robbery crimes in America."

By one industry estimate, more than 1,000 people a day in the United States fall victim to crimes of stolen identity. In 1997 the U.S. Secret Service make 9,455 arrests involving identify fraud. According to the Privacy Rights Clearinghouse there are over 400,000 thefts of identity each year with that result in more than $2 Billion worth of annual losses for the country. Identity theft is expanding at a rate of 50% per year.

Your financial liability is limited to $50. But, your losses will include time and effort to remedy the effects of the theft. You may need to provide extensive documentation to clear up bad credit reports. Some have waited years to clear up fraudulent student loans and fraudulent credit accounts. Others needed to clear up criminal arrest and conviction records.

#10. Insurance for identity theft victims

Identity theft may seem so far fetched but trust me it is not. With today's technology and the growing sophistication of the world wide web, hackers and con artists are now living in a world that used to only exist in the pages of a science fiction book or a scene in a suspense-thriller movie.

This can be a major problem for anyone because not only will you have to worry about your personal properties like credit cards and bank accounts, you also have to think about the fact that someone else is using your name and your reputation to do god-knows what.

According to the FTC, there are more than 160,000 reported cases of identity fraud in the country in 2002.

Identity theft insurance reimburses the victims of identity thefts for the cost of restoring their identity and repairing credit reports. Some companies include these kinds of insurance as part of their homeowners insurance policies while others sell them as stand alone policies or as an endorsementa to a homeowners or renters insurance policies.

On average, these policies cost between $25 and $50 for $15,000 to $25,000 worth of coverage. Identity theft insurance provides reimbursement for expenses such as phone bills, lost wages, notary and certified mailing costs and sometimes attorney fees with the prior consent of the insurer.

Complaints about identity theft have surged from about 40,000 in 1992 to 750,000 in 1998, according to regulators.

Las Vegan Julia Twentyfive knows all too well how identity theft can destroy your life. A thief who stole her purse used her identity to rip off others in a credit card scam. Her nightmare cost her three days in jail, $15,000 and two years of her life to straighten it all out.

Metro police say they receive up to 75 new reports of identity theft every week here in Clark County. It's the fastest growing crime in America today. It's just a matter of time; sooner or later we'll

all become victims.

Ted Burke is a former law enforcement agent who has spent many years dealing with identity theft victims. "They really didn't have an antidote or way to stop the bleeding until we came about. Burke is now the senior regional vice president of Prepaid Legal Services, Inc. in Nevada. His company has offices all over North America and has now partnered with the nation's biggest investigative agency, Kroll Inc., to provide an insurance policy for ID theft victims.

"Generally, we'll find out if they're a victim before they know and we'll notify them," Burke said.

It's called identity theft shield, an around the clock system of monitoring your credit, restoring your identity and reimbursing your costs in case your good name is stolen and used against you. And with 1 of out of every 4 Las Vegans at risk of falling victim to this rising crime, identity theft insurance may be the closest thing our society has to a cure.

Ted Burke adds, "It gives them peace of mind. They can sleep at night knowing we're watching their back 24-7, 7 days a week no matter where they are or what they're doing, we're taking care of them."

Identity theft shield benefits will cost your family anywhere from $10 to $12 a month. Pre-paid legal Services has been in business for more than 30 years and operating in Nevada since 1989.

#11. Dealing with Inevitable Website Scams

The use of computers created advantage in the development of websites. Updates in the latest software as accessories to use in cyber communications, resulted to revolution in the run of business thru the use of the web. It is far more convenient than any existing functions, paves effective, immediate response to the flow of results that goes about in the corporate, as well as the commercial world.

Almost all manufacturing corporations have applied the e-commerce way in trading their productions. In as much as the online services is adapted, emerged the rampant flow of all kinds of thieves to victimize any unfortunate subject inside the e-biz conglomerates.

Hackers, phishers or spoofers operate deceptions by way of scam messages in the websites. The virtual use of pseudonyms makes possible increase of online thieves. They're IT enthusiasts, expert web developers, and adept to latest in software. Most

of them are not successful in their own fields, felt disgusted instead, creating menace in the worldwide website traffic to gain advantage for their own end.

Online theft may act individually, or could be manipulated by a group in one single website name. Survey consortium in the U. S. have developed means to coordinate with the FTC (Federal Trade Commissions) in order to establish a complete record of crime complaints in online deceptions, that starts with scam messages. Surveys show online fraudulent thieves rate at 34% increase from 2004. Households' online spookers' complaints rate 3%, in the U.S., meaning, nobody escapes from these online harassments leading to crime of fraud.

Online phishing happens when a scam message in your internet suggest something into validating your information records in your bank, your affiliate financier, passwords, stating the urgency of the need to update records. Sounds a very valid source but a lot more of a scam message, with the intention of stealing credit lines from your financing sources.

Results worsen, with the complete extracted information taken by this operator, if crime has intensified, against the stolen credentials, he could turn you over to authorities, put you into a pitiful scenario on a very long-termed redemption to financial recovery. With millions of websites worldwide, it's hard to trace the actual culprit.

Answering directly from your end to the website source of the named company, the phisher can make it appear he is in that site, but actually deviates you to another web link.

To avoid this, verify about the message by using landlines that you think is legitimate. Or, answer by using another Internet browser. Never cut and paste any link from the message into your browser. Most of the time, extending links are likely anomalous, or shifting to websites with highly extensive porn settings.

There are countless scams in the web, and it's needless to name them. Always be aware that everybody in cyber is virtually having his own setting for whatever purpose it takes him. The Web is wide open for any kind of good or bad biz intent as almost everybody depicts a persona of anybody, or anything else.

The only sure bet to free oneself of these online deceptions is to protect your site by using security measures like installing anti-virus, firewall, anti-spyware compatible to every platforms that will block your computer from unexpected intrusion. Make sure you are accessing a reputable and certified sites before giving any private information.

#11. Can You Stop Credit Card Identity Theft?

Credit card identity theft can be a very costly problem. In today's world of increasing credit card usage, it is no longer a rare instance where a criminal may be able to make use of your credit card for his own gain. He does not need to have your "plastic" in order to commit such a crime. All he needs will be your number and your personal information. Such a crime has been known as identity theft.

Credit card identity theft can happen in a variety of ways. Almost everyone using a credit card can be an unwilling victim. With all business and financial transactions done through computers and online means, it has made information very valuable as well as very vulnerable to theft. Your personal information has become a very valuable asset.

Anyone who can get hole of it can use it to their advantage at your very expense. Identity theft is basically the act of using your personal information without your knowledge to commit fraud or other crimes. On credit card identity theft, it could mean that such criminals can use your account for their own purchases.

How can such crime happen to someone like you? If you use your credit card on your regular purchases, there are a lot of chances that criminal can get hole

of your credit and personal records. If you handout your credit card to servers at restaurants, you might be making yourself vulnerable to identity theft. If you sign your credit cards, criminals may be able to make use of your signature to commit a variety of crimes under your name.

Your personal information should be on your own safeguard because a lot of crimes can be committed using your own records. It can be as easy as calling your own credit card issuer to change your billing address once they get hole of your credit card information. The impostor can then run charges on your account without you even knowing it because your bills are being sent to a different address.

With your stolen credit information in the wrong hands, impostors may also be able to open new credit card accounts in your own name. When using these credit cards and foot the bill in your name, such delinquencies will be reported on your credit report.

This will make it harder for you to upgrade or make effective use of your own credit account because of your worsening credit record without you even knowing it. It can even go as far as using your name to the police during an arrest. If they do not appear in court to answer the charges, a warrant of arrest can be issued on your name and sent to your address.

Identity theft can be a very disturbing and costly problem. It is all the more important of trying to safeguard your credit information from getting into the wrong hands. You must try not to give your personal information to anybody without checking out on them. Make sure that you trust your personal records only to people and institutions that you can trust. Take the necessary precautions on making sure that you still have control of your credit accounts.

Always be aware of your credit reports and see to it that you are aware of anything out of the ordinary that may come up on your credit records such as purchases that you haven't made yourself. Try to report any discrepancies immediately to the authorities. You can even have your account temporarily blocked in order to prevent further losses.

Do not forget to report it to the fraud agencies in your area so that everything can be done to apprehend and arrest the offenders as early as possible. Remember, the way you give out your personal information can have its corresponding consequences. Always be careful and be on the alert before you ever regret what you might have done.

#13. Beyond Identity Theft Law

In a civilized world, having law to condemn felony is a mainstream practice to protect personal freedom of citizens. Every educated, adult knows the concept of universal right and wrong as far as execution of freedom is concerned like the way no one kills to end someone else's life. As a unique person, freedom means having one identity you claim as yours with ultimate glory. Then one day, you discover someone is using your identity; you freak out: "something is very wrong."

Identity theft law has been passed with customized decree in every federal state. It will give justice to victims whose pieces of private information are abused carelessly by usurpers. Under the "Identity Theft and Assumption Deterrence Act of 1998," it defined how it is a crime to make unlawful use of another person's identification, which is controlled by mandatory requirement to be identified by just using name or Social Security Number.

No matter how many kinds of imposed protection is done to avoid intrusion of privacy through chains of private information through government and non-governmental listings, the problem is sieved by the clever manipulations of the offenders. Free enterprise in the U.S. made this dilemma very rampant in every exchange of business transactions through various means of handling and disseminating cash flow.

Obviously, the best source of private information is through banks and credit cards, where bulks of cash are stored for easy and convenient payment. For unknowing business person, this transgression happens after the theft has successfully caused damage. Identity theft law covers all bounds of these illegal activities through emails, mails and other transaction cards, brokerage, insurance, and other documentations involving membership.

As imposed, identity theft law could penalize villains from 15 to 30 years of imprisonment depending on the degree of fraudulent nuisance done, excluding revoked privileges and forfeiture of assets. Each state has passed legislations to act upon any kind of relevant identity theft cases. Each felony is closely monitored by the federal agency to enforce the law.

Identity theft is a very rampant and not easily toppled crime affecting lives and property of peaceful and law-abiding individuals. Before spending effort on legal suits, why not do preventive measures to avoid waste of time dealing with the consequences of being a helpless victim?

The common saying still prevails: "Prevention is better than cure." It can happen by doing the following measures:

1. Transaction monitoring - this is done by taking

care of the reports of your credit billing by requesting yearly low-charged credit reports

2. Use password wisely - those not easily identified by making it remotely related to you.

3. Be wary of strangers in the house by limiting their access to private information you are keeping.

4. Know the people handling your records in the office/workplace. Make sure to verify how they dispose private information and rule out carelessness in exchanging or disclosing them to other people.

No matter how you take care of your information, there are instances where it slipped off your fingers uncontrolled depending on your daily activities. Just like other ancient crimes covered by the penalties imposed by the law, identity theft is personally damaging to one's integrity. The villains get their share of success because of vile planning in between inefficiency of law enforcement. Don't let this put you into halt with whatever goals you have. Crime will never pay.

#14. Avoid Identify Theft from Obituaries

Identity theft even applies to the dead. Write your obituaries with identity theft in mind because the deceased's identity is an irresistible target for thieves. There are tips that you can follow to avoid identity theft.

Victims of identity theft:

Identity theft of the dead is a deplorable topic to have to discuss, but it must be talked about to help those who may be victims of identity theft in the future. The problem is compounded by the fact that the family is grieving for the dead and being conned at the same time. It is made even worse when the deceased had joint accounts with a partner who is still living because she or he ends up having to pay dearly for the thief's crimes. The saddest part is that the thief often gets away with the crime before he or she is caught.

Identity theft from obituaries:

Con artists will scan the obituaries in their city or town and watch for valuable information that they can use to access bank accounts and personal credit. Long obituaries that give many details give these scam artists more valuable information that they can use to steal the identity of the deceased. The deceased doesn't have to worry about their credit rating, but the family is caused undue emotional stress. Sometimes the thieves want to steal the

identity to avoid immigration, legal or financial problems of their own.

How you can avoid identity theft:

The best way to avoid identity theft from your loved ones obituary is to take care of financial and credit issues before the obituary is published. Close accounts, and notify all creditors, banks and credit reporting agencies of the deceased's passing. The next best thing is to limit the information on the obituary so that there isn't a resume of details that list every occupation, award and detail of the person's life. You can find out more about writing an obituary at www.ObituariesHelp.org

A checklist of what to do to avoid identity theft from obituaries -- If you do all of these things you will ensure that your loved one will not be a victim of identity theft after he or she has passed away. It is even better if you do all of this before you publish the obituary:

Close accounts and credit cards.

- **Notify Equifax, Trans Union and Experian of the deceased's passing.**
- **Contact Social Security and have them deactivate the social security number of the deceased.**

What to do if you suspect identity theft?

If you've already published the obituary and you notice unusual activity on the deceased's accounts, you can assume there is some sort of identity theft and so you must do the following:

- **Notify the police immediately.**
- **Contact your bank and freeze accounts.**
- **Contact credit-reporting agencies.**

The police and credit reporting agencies will have more suggestions for you to keep you safe.

Writing obituaries need not be a daunting task, especially if you have all your financial affairs in order. If you've taken all the steps to avoid identity theft from obituaries, you can rest assured that your obituary can be as long or as short as you would like it to be.

#15. The Identity Theft Quiz

You may think your identity is perfectly safe and

that identity and credit card theft could only happen to someone else, but take a few minutes to answer this Identity Theft Quiz, and see how safe your money and identity really is. Each answer is worth between 1 and 5 points, which you can tabulate at the end of the quiz to see how well your identity is truly protected:

1) What is your primary method of disposal for personal finance information?

A) For the most part, I tear the information up, and then dispose of it. B) I tear some of the information and shred some of it before I dispose of it. C) I use a cross-cut shredder to destroy my documents every time, before disposing of them.

2) What method do you use for disposal of unsolicited, pre-approved credit card direct mailing information?

A) I simply dispose of them in the garbage can. B) I always destroy them in some fashion - either I tear them up, or I shred them. C) I always use a cross-cut paper shredder before I dispose of them.

3) What method do you use to discard other personal information like bank statements, pay stubs, credit card bills, cancelled checks or utility bills?

A)I generally tear the information up and then dispose of it B)Sometimes I tear the information up, and sometimes I shred it. C)I always use a cross-cut paper shredder before I dispose of any of these materials.

4) When do you check your credit report by any of the major credit bureaus?

A)I've never checked my credit report B)I have checked my credit card before, but its been over a year C)In the past year, I have checked my credit report

5) Upon receiving financial statements of any kind (credit card bills, checking accounts, utility bills), do you thoroughly review these statements for any errors?

A)I really don't review my financial statements regularly at all. B)I review my financial statements whenever I can get to it, but not monthly. C)I review my financial statements as soon as I receive them, every month.

6) Where do you get you own personal mail?

A)I use an unlocked mailbox that's right in front of my house. B)My mailbox is lockable, but I don't always lock it. C) I've made sure I have a locked or secure mailbox/PO Box for all my mail

7) What method do you use to send outgoing mail?

A)I always leave my mail in my own, unlocked home mailbox B)I will either leave it in my own, unlocked mailbox with the flag up, or occasionally drop it off at a secured mail drop box. C)I only drop my mail in a locked mailbox, or US Mail collection box.

8) Do you ever carry your Social Security card in your purse or wallet?

A)I do carry my Social Security card with me on a regular basis. B)I don't always carry my Social Security card, but sometimes I travel with it. C)I never bring my Social Security card with me. I store it in a safe place.

9) Is your Social Security number included on any personal information you carry with you? (Checks, ID cards, health-insurance or prescription drug cards)

A)I really couldn't say. I haven't noticed. B)My social security number is on several of my ID or

insurance cards. C)No, I don't have my social security number on anything that can be found on my person.

You can calculate your score using the following key: A=1, B=3, C=5. A score of less than 20 means that you might be at real risk for identity theft. A score of 20-37 means that you have begun taking the right steps but you can still improve. A score of 38-45 means that you are doing the right things to protect your identity. However, you still need to be careful because it only takes one piece of information to end up the wrong hands to result in your identity being stolen.

#16. How To Prevent Identity Theft By Computer Hackers

Preventing Identity Theft is the best identity theft insurance.

This also applies to computer hacking because there are clearly ways to prevent identity theft from this method. Many have assumed that the incidence of identity theft would have decreased with modern technologies as an identity theft shield, but in fact, researchers on identity theft, report that there is a rise in Computer Hacking, which also often leads to the theft of someone's identity. One in twenty Americans are victims each year, which is a staggering number of people lives that are turned

upside down, because their personal information ended up in the wrong hands.

What is computer hacking?

Computer Hacking is a process that is used by individuals that are skilled in technology and know the necessary techniques to access other people's personal information that is either stored on their computer or a company's computer network. Computer Hacking is something that has serious consequences for those that are caught because they can spend many years in prison. Many hackers go straight for corporations in an effort to gain access to multiple personal financial records, while others stay on a smaller scale with individuals so they are less likely to be detected.

What is a wireless network?

A computer wireless network (Wi-Fi) is one in which data is transmitted using radio signals instead of cables. Typically, wireless network has one or more computers that connect to the Internet via an access point, which is typically a type of router that is the gateway for the computers on the network to connect to the Internet. One of the ways you can Prevent Identity Theft when using a wireless network is to ensure it has the proper security features on it are operational. Home or office Wi-Fi with a WPA2 encryption service that is not internally shared

provides the best security. If you have this facility you are less likely to become a victim of Computer Hacking.

What is computer identity theft?

If you have personal information stored on your computer or use your computer to buy items over the Internet on an unsecured wireless network, you can be subject to Computer Identity Theft. This happens when the thief engages in Computer Hacking and is able to obtain your credit card information, social security number, and other personal information, and then poses as you to take on your identity, or simply to access and withdraw funds from your bank account(s).

Why are wireless networks so vulnerable to hackers?

The biggest reason that wireless network is a stomping ground for Computer Hacking is that many people use open networks. Open networks are those at coffee shops or airports that have no special security on them or home or business networks that do not use WAP2 encryption service for their network. This means that everyone can connect to this network because it has no security key and wreak havoc on those that are connected to it. The best way to Prevent Identity Theft, is to have your own security system on your computer before you ever connect to an open wireless connection.

What you need to know about wireless internet security?

Many companies and individuals work wirelessly and it has become more popular because it does not require your computer to be wired to an Internet connection, but operates by wireless signals to the router. You should be aware that there are ways to Prevent Identity Theft when you are working wirelessly. When you are working at your place of employment wirelessly, you are under a lot of wireless security and therefore safer from Computer Hacking. However, when you go to public places where there is a lot of sport or a wireless connection that you can join, you risk Identity Theft because the security is turned off, which means all the information you are sending via the Internet can be seen by anyone by someone with hacking software. Security measures are your best way of staying safe from those that are looking to steal someone's identity. There is a software add on to a popular internet browser that allows hacking into other user's information in an unprotected Wi-Fi network.

How you can prevent computer identity theft with a wireless computer network?

Wireless networking is definitely here to stay and you will use it at home and at your place of business, but you can Prevent Identity Theft by being smart

about how you use your connection. Frist, make sure you have a secured wireless network set up at home, so that no one can connect to the network without the special key that you set up. Secondly, ensure that your work participates in high wireless security so that you can be safer from Computer Hacking. Lastly, watch out for public and free wireless access hot spots since these are unsecured and sending personal information over an unsecured network is like playing with fire. If your work involves a lot of travel and use by laptop of public Wi-Fi networks you should have a virtual private network.

You can do a web search to find the best companies -- just type in 'Virtual Private Network' that will help secure your data.

#17. Identity Theft is Still at Large

Though it may seem like something that does not affect many people anymore, since we all know so much about the issue now, many people in America are still affected by identity theft today. Even though we know more today about the dangers of identity theft those who seek to steal identities are constantly trying to find the next new technology that will help them get around our current security measures. The Justice Department released figures about the number of households affected by identity theft last

year. A staggering 8.6 American households had at least one member in the home over the age of 12 whose identity had been compromised last year. That number is an increase from only 6.4 million in 2005.

Not only are identity thieves still doing a booming business, they are making more money than ever. The Justice Department stated that American households suffered upwards of thirteen billion dollars last year alone! And those are direct financial losses, which means that's money that these families will never see again.

According to officials, the majority of the increase in identity theft loss happened from the misuse of credit cards. The numbers of people using ill-gotten personal information to open new accounts actually decreased in the five year period from 2005-2010. And even though overall American households lost over thirteen billion in 2010, twenty four percent of those who experienced identity compromise suffered no direct financial loss. Unfortunately even though that sounds positive, it means that the other seventy six percent of the people affected by identity theft in 2010 took on all of that thirteen billion dollars by themselves.

Identity theft can happen to anyone, and when it does the effects go far beyond what many expect them to. Even if you are a victim there are certain situations where you can be held liable for financial losses due to identity theft. Usually if you have only been

scammed out of your credit card information you will probably only be held liable for the first fifty dollars in damages. That can be a lot of money for some, but it doesn't compare to what can happen if thieves have their hands on some more pertinent information. If you lose your debit card information for example, especially if you've also lost the PIN number, you can be held responsible for most if not all the illegal charges to your card. It's not unheard of for thieves to get their hands on a debit card and PIN and then wipe the accounts clean and then some, leaving the victim to pay any overdraft fees.

And when you consider the myriad of other ways a thief can steal your identity, it can be a daunting task for some families where they are left struggling to pick up the pieces. There can be cases where someone steals your social security number, your tax information, your insurance information and people can even provide your stolen information when they commit a crime thereby placing a warrant out for your arrest! Though these situations are less common that credit card and debit card theft, they do happen and the effects can be much more devastating than missing your life savings. Many victims of identity fraud have to invest countless hours and their own personal money into not only restoring their accounts; But restoring their good name -- they are tasked with spending the time and money to restore their credit and potentially their criminal record too.

#18. Tax Season is Bringing Out Identity Thieves

Overviews identity theft tactics such as Spoofing, Phishing and Pretexting as a means to steal identities. Covers means to protect ones identity and recommends review of free annual credit reports and the services of a proactive identity theft protection service.

A number of clients have recently reported to their tax preparation services that they have been receiving calls from someone posing as a representative from the Social Security Administration. The caller began the conversation by talking about the pending Congressional leader's announcement where a deal with the White House on the economic stimulus package would give most tax filers refunds of $600 to $1,200, and more if they have children. The caller went on to solicit from consumers their Social Security number stating confirmation of their number would ensure they received their rebate checks within the next 6 - 7 months.

The Social Security Administration is not making a conscience effort to confirm consumer identification numbers. You need to be aware that identity thief's are however and they use a number of tactics to steal your identity. Spoofing is generally used by thieves as a means to convince

individuals to provide personal or financial information that enables the perpetrators to commit credit card/bank fraud or other forms of identity theft. An attempt to fraudulently acquire sensitive financial or personal information, such as credit card information or a Social Security number, by impersonating a business representative or trustworthy person is also known as a Phishing attempt and is usually initiated through e-mail, phone calls or Instant Messaging.

Thieves do not just collect Social Security Numbers. They are also after your telephone records, date of birth and your bank and credit card account numbers. This information is a personal asset as well and people who illegally solicit this information are also known as pretexters.

It is yet another name for identity theft and Pretexting is (like the other practices mentioned) a means of getting your personal information under false pretenses.

Pretexters sell your information to people who may use it to get credit in your name, steal your assets, or to investigate or sue you. Pretexting is against the law. Whether it is by means of Spoofing, Phishing or Pretexting the tactics are all designed to get your personal information.

According the Federal Trade Commission For example,

a pretexter may call, claim he's from a survey firm, and ask you a few questions. When the pretexter (let's just call it a thief) has the information they want, it is used to call your financial institution.

The thief pretends to be you or someone with authorized access to your account. They might claim that they have forgotten their checkbook and need information about their account. In this way, the criminal may be able to obtain personal information about you such as your SSN, bank and credit card account numbers, information in your credit report, and the existence and size of your savings and investment portfolios.

Keep in mind that some information about you may be a matter of public record, such as whether you own a home, pay your real estate taxes, or have ever filed for bankruptcy.

It is not pretexting for another person to collect this kind of information. Identity thieves don't just use the schemes we've just talked about to get your personal information they also procure your identity by:

*** Stealing wallets, purses and your mail (bank and credit card statements, pre-approved credit offers, new checks and tax information);**

*** Stealing personal information you provide to an unsecured site on the Internet, from business or personnel records at work and personal information in your home;**

*** Rummaging through your trash, the trash of businesses and public trash dumps for personal data;**

*** Buying personal information from "inside" sources. For example, an identity thief may pay an employee for information about you that appears on an application for goods, services or credit.**

Even though the laws are on your side, it's wise to take an active role in protecting your information. The Federal Trade Commission recommends the following actions;

1. Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or know who you're dealing with. Pretexters may pose as representatives of survey firms, banks, Internet service providers and even government agencies to get you to reveal your SSN, mother's maiden name, financial account numbers and other identifying information. Legitimate organizations with which you do business have the information they need and will not ask you for it.

2. Be informed. Ask your financial institutions for their policies about sharing your information. Ask them specifically about their policies to prevent pretexting.

3. Pay attention to your statement cycles. Follow up with your financial institutions if your statements don't arrive on time.

4. Review your statements carefully and promptly. Report any discrepancies to your institution immediately.

5. Alert family members to the dangers of pretexting. Explain that only you, or someone you authorize, should provide personal information to others.

6. Keep items with personal information in a safe place. Tear or shred your charge receipts, copies of credit applications, insurance forms, bank checks and other financial statements that you're discarding, expired charge cards and credit offers you get in the mail.

7. Add passwords to your credit card, bank and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.

8. Be mindful about where you leave personal information in your home, especially if you have roommates or are having work done in your home by others.

9. Find out who has access to your personal information at work and verify that the records are kept in a secure location. Checking your credit report annually can help you catch mistakes and fraud before they wreak havoc on your personal finances.

Order a copy of your credit report from the three nationwide consumer reporting companies every year. To order your free annual report from one or all the nationwide consumer reporting companies, call toll-free 1-877-322-8228, or complete the Annual Credit Report Request Form avail at their Website annualcreditreport.com, and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

If you do not have the time or expertise to put measures in place to protect you and your family's identity consider visiting a credit protection service that can put the appropriate measures in place to preserve your good name, credit and assets.

#19. Identity Theft And The ATM Game

No matter what kind of advancements in technology identity thieves will always find a way to exploit it. The ATM is a prime example.

They were supposed to be of such great convenience and in truth they really are. The automatic teller machine has been a godsend to many of us. Stranded in a remote area? Chances are there is an ATM there for you. Got to get some quick cash and three o clock in the morning? No problem. As a matter of fact it is a whole lot easier these days to find an ATM then it is a pay phone which seems to be going the way of the buffalo.

All of this is just fine with identity thieves. Name the device and the odds are identity thieves have a scam for it. And when it comes to the automatic teller machine they have hit the proverbial jackpot.

How much of a jackpot? At the very least over one billion dollars and as of this writing shows no signs in letting up. Law enforcement officials in some parts of the country are reporting an increase in ATM fraud activity.

So how do scammers go about pulling off these elaborate yet highly effective rip-offs? There are a number of ways but a few make it to the top of the

list:

1. The Skimmer

Skimmers are small electronic devices which can be place directly inside the ATM. If you think it should be something that anyone can easily detect think again. People go to an automatic teller machine to get money not to ponder whether or not someone is trying to rip them off. Therefore the chances are if you are not looking for it you will not see it. And many experienced identity thieves no how to hook it up in such a way that even if you were searching for it you would not find it.

The skimmers job is just that. To glean as much information off your card as possible once you put it into the terminal. That information includes the card number, the expiration date, the CVV and pin number. It's the equivalent of you telling a total stranger all of your credit card and financial information. In Staten Island a group of thieves got away with over a half a million dollars using skimmers in conjunction with miniature cameras.

2. The Shoulder Surf

From time to time in your search for an ATM you may come across a line of people who had the same idea as you. Yet every now and then somebody standing in

that line has a different idea and that is to steal your information.

Now shoulder surfing on its own is not the issue. If the thief does not know what your card number is then it does not matter how many times they watch you put in your pin number. But if they have installed a mini camera to capture your information then that's a different story altogether.

Keep in mind it doesn't have to be anything high tech. Placing some kind of adhesive in the card slot like glue or even bubble gum will suffice as long as the card gets stuck to the point you either have to keep typing in your PIN or you are totally unable to retrieve it.

Then it all comes down to timing. Identity Thieves hope you leave the scene for enough time for them to get what they need and disappear. Going into the bank lobby to report what just happened is one way to ensure they are successful.

ATM's are not just confined to bank machines either. They are used at gas pumps, restaurants, supermarkets and anywhere else they are required. That by no means implies everyone is out to steal your identity. It does mean however that you should be extra cautious and observant when you go to use an automatic teller machine no matter where it is.

#20. Identity Theft: Up In A Down Economy

A lot of people are hurting in what has become a global recession. Identity thieves could not care less. As far as they are concerned business is booming

Turn on your TV and no doubt you will have seen one or more talk show hosts chatting it up with an economist or historian. The reason you may be seeing a lot more of these folks is of course due to the tough economy. Both groups agree that we are not at the Great Depression levels of the 1930's but we are no doubt experiencing problems which in many ways are comparable to that time period.

Wall Street is tanking, foreclosures have exploded and many businesses are out of business or at least not far off from shutting their doors permanently. A huge chunk of the population is hurting and what makes the pain even more severe is that identity theft is on the rise.

This is an unfortunate reversal of fortune. While identity theft has been ranked as the number one consumer complaint for nearly a decade, the reports of identity theft had actually been declining. This can be attributed to people better educating

themselves and taking the necessary safeguards to decrease their risk. Some specific numbers while not a cause to hold Mardi Gras celebrations were very encouraging.

For instance according to Javelin Strategy & Research, the amount of money loss to identity theft victims declined by about twelve percent. This goes hand in hand with another statistic; namely the amount of money spent to fix the problems caused by the initial theft went down by thirty one percent. In about half the cases, identity theft victims did not have to shell out any money at all.

This is all good news but it looks like the dark clouds are moving back in our direction and we probably have the financial crisis to thank for it. James Van Dyke is president of Javelin Strategy & Research. When asked by CNN about the sudden turn around he stated, "The only thing we can logically attribute that to is the economy. If people need to make money, and decide to do so illicitly, identity fraud is the logical opportunity."

Why is identity theft the logical opportunity? For the simple reason it utilizes an ever growing variety of methods which are so easy to get away with. And it also does not hurt that there are no one hundred percent safeguards available.

We have been warned by many experts and public

officials that times could get decidedly tougher and stay that way for the near future. That means belt tightening and making some hard choices in our personal lives. It also means that the last thing any of us can afford right now is to leave the door open for friends, acquaintances, relatives or total strangers to take advantage of a logical opportunity.

#21. Think You Don't Need a Shredder? Think Again

With identity theft ever on the rise, no home can afford to be without a paper shredder. Identity thieves are both persistent and creative, and they have no qualms about going through your trash to get what they need. You may be surprised to find that it is perfectly legal, in fact, to go through someone's trash!

What can you do to protect yourself and your confidential documents? Well, if you have been avoiding buying a personal paper shredder because you don't know what to look for, you should probably get over that right now. Here are a few things to keep an eye out for when you are shopping shredders.

Shred Pattern:

When it comes to shredders there are really two different kinds: the kind that cuts documents into several long strips (known as strip-cut shredders), and the kind that cuts them into confetti-like shreds (known as cross cut shredding). For shredding confidential documents which could prove damaging were they to fall into the wrong hands - such items as bank statements, junk credit card offers, credit card statements, and tax records, we really can't recommend that you use anything but a cross cut shredder that is rated at a Security Level of 3. If you can't find the security level on the box, or your salesman doesn't know, you can pretty much rest assured that most any cross cut shredder is a Level 3. Just to be safe though, the particle measurements listed on the machine you are shopping should be no larger than one-quarter inch by an eighth of an inch.

There are shredders that have Security Levels up to 6 (for top-secret government documents), and you may have your reasons for considering a Level 4 or 5 machine, but for the purposes of a home shredder, in the majority of cases, Level 3 should be plenty.

Sheet Capacity:

For the purposes of a small office or home use machine, you should expect to be able to find a cross cut shredder that can handle from 6-8 sheets at a time with no problem. There are a few other features you might want to keep an eye out for, such as the ability for your machine to handle paper clips and

staples, a reverse function to help in preventing paper jams, and an automatic on and off function that turns the shredder on when paper is placed in the feed, and turns it off again when the job is done.

The key to personal shredding and to working with the lower capacities you will find in the smaller machines is to shred daily, or on an as needed basis, rather than letting your papers pile up and trying to shred them all at one time. Smaller shredders have smaller motors and thus they are more prone to overheating if overused. Your shredder should come with usage recommendations so you can keep within the correct range for your machine.

Maintenance:

The cutting heads of shredders need to be oiled on a periodic basis. There are several ways to do this, but the best is probably to squirt a zigzag pattern of shredder oil onto a normal piece of paper and run it though the shredder, then hit reverse for half a minute or so.

#22. The Young Victims of Identity Theft

Looks at the growing epidemic of identity theft associated with minor children and young adults.

Article points out proactive measures to take to avoid identity theft. Provides contact information to credit bureaus to obtain credit histories and directs people to credit services that safeguard identities.

According to the Federal trade Commission there was an estimated half million children who joined the ranks last year with the unfortunate distinction of becoming victims of identity theft. An advocacy group called the Identity Theft Resource Center identifies relatives as being involved in more than half of the child identity theft cases reported in the United States in year 2006.

It should be noted however, the thief is not always someone who knows the child. It is suspected by this resource center that identity theft of children is increasing so rapidly precisely because kids are such good targets. They further believe children are victimized because they usually have a spotless record and because they aren't using their credit and as such; the crime can go undetected for years.

Now that most infants by law have social security numbers, thieves have discovered they may be the easiest targets of all. Thieves have years to manipulate these identities and create a considerable amount of damage. Infants and children remain lucrative targets because they typically don't use their social security numbers until their late teens and discover the theft problem upon

applying for a first job, a student loan or a credit card. When families and their children finally find out, the burden of proof falls on them.

Some of the most common tactics of identity theft (but not limited to) include parents using their children's' Social Security numbers to open up new credit accounts, and "dumpster diving" thieves stealing credit offers mistakenly sent to children too young to make use of the application themselves.

Helen Simmonds, a detective in a local police department, has been handling identity theft investigations. It was noted that almost all involved Social Security numbers issued in the early 1990s to children who are now turning 16, 17 and 18, and trying to obtain credit for the first time. It is believed by the investigator that there is going to be an epidemic [of such cases] not just locally but; across the nation.

It then should come of no surprise that credit-monitoring services are beginning to target concerned parents, offering to monitor children's identities. At LifeLock, credit monitoring for your child costs only $25 annually in addition to a $10 monthly charge for adults. LifeLock also takes actions to basically audit the Social Security Administration annually on the child's behalf to find out if there's been any work history related to the child's identity number.

A spokesperson for the SSA advises that parents can simply call their local Social Security office and get that information free of charge. However as a concerned consumer and parent you need to know; if thief is using your child's Social Security number, but with a different name then your child's, the SSA will not find a matching record for your offspring.

One of the major credit reporting agencies: Experian - recently launched FamilySecure monitoring service which alerts parents as soon as anyone applies for credit using their child's name. However, at $19.95 a month, the cost might be a bit cumbersome to many family budgets.

Parents that remember or have the time whom want to contact the three Credit Bureaus to determine if there is any activity on their children's credit can use the following contact Information and procedures;

Experian Call 1-888-379-3792, select the Fraud option. Parents have to mail in documentation, including proof that they are the parent or legal guardian for the child, such as a birth certificate for the child and driver's license for the parent. If the child does not have a credit file, Experian will notify the parents in writing. If a credit file exists, Experian will provide a copy to the parent so they can dispute any fraudulent information. The

bureau will attach a notice on the file that it belongs to a minor, to prevent lenders from issuing credit in the future.

For Equifax Mail a request to: Equifax Information Services, P.O. Box 105139, Atlanta, GA 30348. Attach documentation identifying you as the child's parent (see above). If a credit record exists, Equifax will delete any fraudulent accounts, take the report offline and flag the Social Security number as one belonging to a minor. Parents cannot receive a copy of the fraudulent report.

Actions for TransUnion require a parent to Email childidtheft@transunion.com TransUnion will email back instructions on requesting a file. If one exists, the bureau will lock the file until the child turns 18, so his or her information cannot be used to obtain credit.

TIPS for ID Theft Prevention:

Don't give out personal information: never reveal anything about yourself unless you initiate the contact or if you request a phone number that you may call back to authenticate the representation being made (do not give out your Social Security number, phone number, date of birth, or credit card numbers or carry your Social Security Card).

Watch your mail: make sure you collect it right after it is delivered if it is out in the open and accessible to others.

Shred important documents: SSN, credit card numbers, driver's license numbers, date of birth and pre-approved credit offers (you can stop these by going to.

Pay attention to your billing cycle: missing bills could indicate theft.

Use reputable and secured websites: always use a secure browser, when paying online check to make sure it's secure (https: instead of http: identifies a secured server that encrypts the information you submit).

Protect your PC: protect against viruses and spyware, use a firewall, and don't download attachments from people you do not know.

Do not carry your Social Security card or that of you children's in your walletFree Web Content, purse or automobile. Secure the cards in a safe place when not specifically needed.

There are services that charge for protective and proactive identity measures to safeguard the good

name and credit of adults and minor children. If you do not have the time or expertise to put needed safeguards in place make room in the budget for the available experts.

Thief's have the time and ability to steal and ruin your identity. Don't think for a minute it can't happen to you or your family members because millions of others were just as confident and lost.

#23. Identity theft and fraud criminals are turning their attention to senior citizens

If you have a senior member of your family, you can help them to become aware of identity theft and show them what they can do to protect their identity and fight this growing crime.

A lifetime of savings may be safely sitting in a bank account to take care of retirement years. Identity thieves know they can steal that money in a matter of minutes if they can convince a trusting older person to disclose sensitive data. Most seniors grew up in a time where trust was very important, and it was rude to question a person's motives. Times have changed, but most seniors are still very trusting. Unfortunately, criminals are anxious to turn that trust into a nightmare. If you have a senior member of your family, you can help

them to become aware of identity theft and show them what they can do to protect their identity and fight this growing crime.

Seniors And Technology:

Seniors have fallen in love with technology just like everyone else. They enjoy the email that allows them to contact friends right away. It's especially nice to have the convenience of email when the weather is cold or snowy. Seniors also love social media. It puts them back in touch with friends that moved away years ago. Photos of children and grandchildren are treasures to post on social media pages and share with friends. Many seniors, however, are not really technology savvy and are not aware of all the dangers that can befall them online.

Encourage your senior to buy a paper shredder, or buy a shredder for them if they are concerned about the expense. Explain that just tearing pieces of paper in halves or quarters is no longer a safe option. Teach them to become ardent shredders and then the shredded paper can be distributed to recycling centres.

Explain that it is not safe to store any important data in their wallets or handbags. ID cards, benefit cards, passwords, PINs, and other sensitive information should be kept in a drawer or cabinet that can be locked. If they are unable to memorize their passwords, they can be written in a small notebook that is also kept in the locked location. Have your loved one keep all their credit papers and contracts in the same locked place, and ask for a key for yourself in the event he or she loses theirs or if they are away on a trip and need you to access some information.

If your senior is using online banking, teach them how to identify a secure site. On a secure site, the "http" will have the letter "s" in front of it, as in "shttp//www". Secure sites also display a small yellow lock in the lower toolbar section of the page.

Email is another area where identity thieves can target seniors. The practice of "phishing" deceives many people, not just seniors, into giving away personal information without even knowing it. The "phishing" emails will usually appear to come from a bank or credit issuer. Instruct your senior to delete all mail from any bank or creditor they do not do business with, and to never log into any kind account through a link in their email even if appears to be a legitimate email. Banks seldom include a link in their emails. Your senior should login to his or her bank or other credit account through their browser. If there is important information the bank wants customers to know, it will be on the web site.

Assist your senior with monthly balancing of bank and credit statements. Look for any discrepancies. Also check credit reports on a regular basis and look for suspicious activity. It's important to catch a thief's attempts at establishing credit in the name of your loved one. Contact any organisation where an attempt has been made and be sure they know it was not the account owner making the credit applications.

It is very difficult to think of your loved ones being separated by the death of one. Unfortunately, that is a time when criminals like to prey on the survivor. Identity thieves scour the obituary columns looking for information they can use to establish a new identity. Resist the temptation to include more than a small amount of non-personal information in the obituary.

There is no reason seniors should not be able to safely go online and enjoy the social aspects of the Internet. Their trusting nature must be just a little less trusting in order to protect their identity and keep their personal information safe. By following the suggestions they can have their money in the bank and not in the pocket of a thief.

#24. What is Business or Commercial Identity Theft?

Business or commercial identity theft happens when thieves use an existing business' name to get credit, or they may bill a business' clients for products and services. Sometimes the Social Security number of a company's officer or another representative is required to commit business identity theft.

A big problem is that identifiers, such as federal IDs or employer identification numbers, are readily available in public records, dumpsters, or internally at banks and other creditors—which makes the ease of access to these numerical identifiers a catalyst for business identity theft. Business identity theft perpetrators are often former employees or current employees with direct access to the books and other forms of financial documentation. These schemers have ample opportunity to pad the books in favor of fraud.

Business identity theft victims don't usually find out about the crime until big-time losses accumulate, or an audit occurs and someone discovers discrepancies on the books. Because of the hidden nature of the transactions, businesses can lose vast amounts of money. Business identity theft can remain undetected for years.

How can you protect yourself from business or commercial identity theft?

Inside job:

Business identity theft, or commercial identity theft, is an inside job. Employees often have access to documents that include owners' and board members' Social Security numbers, as well as the business' tax ID number.

Need-to-know basis:

This information must only be accessed on a need-to-know basis by employees with proper credentialing. Even then, be suspect. It is imperative that this information stays secure.

Checks and balances:

Organizations should put a check-and-balance system into place, ensuring that for every employee who has access to company accounts, there are two employees—preferably upper management—who are assigned to make sure the books are balanced, that no money is missing, and that financial statements are double-checked for inaccuracies.

Forensic accountants on retainer:

In some instances, it is necessary to contract with forensic accountants or examiners to pay close attention to a business' books and work to put monitoring systems in place.

Identity theft protection:

Identity theft protection can be a helpful tool to keep officers or owners informed of potential illicit activities, because a Social Security number is often required to open accounts under a business' name.

#25. Can Vacationers And Business Travelers Be At Greater Risk Of Identity Theft When They Travel?

Over seven million people in the United States last year alone were victims of identity theft resulting in almost fifty billion of fraudulent credit card, bank, and other financial charges. A significant number of these victims were tourists, business travelers, and people on their holidays. Here is some valuable information that may save you a ton of grief when you travel.

It's very easy when people travel on their vacation to let their guard down. They have a lot on their minds remembering everything they need to take care of before they go and what they need to take with them on vacation. Not only that, they want to relax, unwind, and have fun. Isn't that what vacations are suppose to be all about? When they travel they don't want to have to be on guard all time and constantly concerned about getting ripped

off every second of their holidays.

There are three major sources of identity theft that you should be aware of when you travel. Your wallet, your laptop or PDA, and internet cafes.

Research shows that most identity thefts occur when people's wallets are stolen, usually by professional pick pockets. Whether you travel on vacation or business you must guard your wallet at all times because you are at more risk than in familiar surroundings. Never carry your wallet in your back pocket - it's not called the "sucker pocket" for nothing. It's best to carry your wallet in a fanny pack. Some travelers prefer a fanny pack with a Velcro closure instead of a zippered one because you can hear it being opened. The usual places you find pickpockets are in crowded areas such as airports, train and bus stations, hotel lobbies, restaurants, and sporting events.

Most people carry more personal information in their wallets then they need. The first thing that you should do before you travel is to go through your wallet and take out any personal information items that you don't need when traveling such as bank checks, check books, credit card receipts, bills, and memberships cards such as library cards. You also don't need to take your social security card as you probably have that number memorized by heart.

Debit cards are a convenient way to take small amounts of cash out of ATM's when traveling, but are also a great way for thieves to clean out your bank account if they get a hold of them. One way to reduce this risk is to open up a separate account at your bank before you go and only put as much day-to-day cash in it as you think you may need for your holidays. Take only that debit card with you.

Credit cards are protected by Federal law so are a much better choice to take with you as you are generally covered for any fraudulent charges incurred. Also, if you are over-charged or find an error on any of your credit card transactions when traveling, it's easier to get the charges corrected or reversed from the card companies. You probably should take two credit cards in case one is lost, or compromised. You can obtain smaller, limited amount prepaid cash cards from Visa, MasterCard, and American Express that are perfect for daily use. You can get these cash cards in any denomination. It is probably best to get a couple of cards with low limits of five hundred dollars or less each. If they are lost or stolen, the credit card companies will replace any pilfered funds. Leave your major cards and passport in your hotel room safe or the hotel's safe along with any other personal information that you do not need from day to day.

Before you travel be sure and check that your credit cards do not expire while you are on vacation. And be sure to call your credit card issuers and let them know when and where you plan to holiday so they don't

have a seizure or conniption fit and cancel your card when they see a credit charge appearing from some place like Timbuktu. Make a note of these phone numbers and take them with you on vacation.

Another major source of identity theft starts with a stolen laptop. Over six hundred thousand laptops are pilfered in the U.S. alone, frequently from inattentive travelers in airports, restaurants, and hotel lobbies.

Before you travel, backup your laptop and put the backup disc in a safe place at home or in a safety deposit box at your bank just in case your laptop is lost or stolen. Put a small strip of colored tape on the top and bottom of your laptop and laptop case as most laptops and their cases look similar in appearance. Write your name, destination address, and contact information at you destination on a piece of paper and tape it to your laptop just in case it's lost at the airport. You shouldn't use your home address on this piece of paper. It's better to use your work or business address and phone number. There are so many laptops left behind unintentionally. The lost and found office at airports do not have time to try and gain access to all the laptops which are more than likely password protected anyway.

The third major source of identity theft can happen at any public computer or internet cafe. Your personal information could be at risk even if you

are just accessing or sending e-mails. A key stroke logger could be installed which secretly keeps a record of all user names, passwords and personal information entered on the computer. Even if public computers are not compromised they still store the information you input in the temporary internet files and history. Never access any bank or credit card account, or pay bills from these computers. In general, computers located in the business centers of hotels and on cruise ships are safer to use than other public computers.

#26. Will Obamacare Lead to Identity Theft?

The fear mongers and Obamacare haters make a scary point and want you to know that as soon as the Patient Protection and Affordable Care Act goes live, your identity will be at risk and, more than likely, stolen. Forbesreports in regard to what's called the Obamacare-mandated "data hub" in which personal records are exchanged among seven different agencies—the Internal Revenue Service, the Social Security Administration, the Department of Homeland Security, the Veterans Health Administration, the Department of Defense, the Office of Personnel Management and the Peace Corps."

Obamacare is required to protect our data under the National Institute of Standards and Technology guidelines. However, naysayers believe the

administration will open the system without proper security certification because Obama will offer a waiver.

It is scary enough that seven different agencies will have the data on file—and scarier still that the possibility of a waiver being granted is very possible due to the enormity of the project.

Right now, pre-Obamacare, your personal identifying information is being shared or stored amongst dozens or potentially hundreds of organizations that you have interacted with since birth. So what's the big deal with another seven? Unfortunately, it's another touch-point where your information can be viewed, hacked and stolen.

My suggestion: Don't worry about it. Seriously, don't worry about it. However, you must DO something about it and I have two suggestions:

- **Get a credit freeze. Search "credit freeze" and the name of all three credit bureaus separately. Freeze your credit. But that's not enough.**
- **Get identity theft protection. I have a credit freeze and identity theft protection. With these multiple layers of protection, my data is next to useless to a thief.**

#27. iPhone Data Security : What you Need to know

iPhones enable us stay connected. However, with personal data being exchanged over the internet, your identity is most certainly at risk. To prevent falling victim to identity theft, you have to take certain precautions, such as protecting your private folders with folder locking software.

iPhones can basically do everything your computers can, the difference is that you can carry your iPhone wherever you go. You can check your email, take pictures, and watch movies, surf the internet, and video chat with loved ones using your iphone.

However, the more we become dependent on smart phone technology, the more we are at risk of having our identities stolen. When we surf the internet using our iPhone, we often don't realize that the wifi connection may not be encrypted; as a result we carelessly conduct transactions over the internet and unknowingly expose information related to our identity.

According to statistics, 12 million Americans had fallen victim to identity theft in 2011, 13% more than 2010. The reason behind the rise in this

statistic was that Americans are becoming more careless about using their smart phones. According to legal experts, if your phone is lost with personal information stored on it and you became a victim of identity theft as a result, then your options are limited. In fact, in some extreme cases, the victims had to file for bankruptcy due large transactions made by identity thieves.

Nevertheless, if you believe you may have fallen victim to identity theft, you can take the following measures to prevent ID thieves from ruining your credit.

First: Place a fraud alert on your credit report, Second: notify your bank and credit card companies, Third: File a report with the local police, lastly, file a report with the FTC (Federal Trade Commission). Taking these measures will put authorities on alert and on the look-out for suspicious and fraudulent activities originating from your personal details. Moreover, to minimize your risks you should limit or stop using your iPhone on public wifi networks, run a virus scanner periodically on your iPhone and finally, keep a pass code on your iPhone.

However, the latter security measures is not fool-proof and expert hackers can easily bypass your pass code on your iPhone and retrieve personal files and folders that contain documents related to your identity. To combat this issue,

your only option is to install an iPhone file security software such as Folder Lock for iPhone. With this software, you can select your most personal files and folders and add password protection on them. As a result, anyone trying to access your personal files will be prompted to enter a password.

The beauty of iPhone file security software is that its hack proof. It uses the latest in file security standards which blocks any hacking attempts. So if you have taken all the above mentioned files security measures and protected your personal files and folder with Folder Lock with iPhone, you're not likely to fall victim to identity theft.

#28. Does Lifelock Work?

Its the question I seem to get asked more than any other on my identity theft blog, "Does Lifelock work?"

This eook explains why I believe it does.

Does Lifelock work seems a popular question on the security forums nowadays and to answer it we need

to look at a few official numbers. For every one million Americans the Government expect 30 000 to be a victim of identity theft. Lifelock has around one million customers and so far less than 80 of them have had to make a claim on their guarantee. I'd say those figures pretty much prove conclusive that Lifelock does work but if not, there is more....

How does Lifelock work?

Lifelock works by placing fraud alerts on your credit files on your behalf. This means that any company who does a credit check on you causes a red flag to be raised and you are informed. Credit checks are carried out when someone applies for credit, a loanScience Articles, a credit card etc. Lifelock also ensure your name is removed from mail lists as the less your details are spread around the less chance of them falling into the wrong hands.

How well does Lifelock work compared to other identity theft protection companies?

Lifelock stops your identity from being stolen where as other identity theft protection companies such as IdentityTrust monitor your credit and report unusual activity to you AFTER the event. Because Lifelock place a fraud alert on your credit file the only way possible for

someone to misuse your name to gain credit is if the provider of the line of credit did not do a credit check and because identity theft is now a major problem (its the fastest growing crime in America) this is very unlikely to happen.

Does Lifelock work with credit experts because i have heard I can do everything that Lifelock does all for myself and save some money?

Lifelock use experts who know exactly how the system works and make sure your fraud alerts are in place at all times. The 3 credit bureau's don't like you to place a fraud alert against your name and they certainly do not like your name being removed from mail lists as it is the sale of these lists that make them so much money. For this reason they don't make it easy for you to do it yourself. Each alert only lasts a certain amount of time and for it to be effective you cannot let it lapse.

You certainly could do the work yourself just as you could walk to work this morning. Question is why would you walk when you have a car and why would you take it on yourself to protect your own identity when Lifelock can do it for a few cents a day. Perhaps the answer to the original question Does Lifelock work? should have been yes because Lifelock gives you peace mind. They take care of dealing with all the credit bureau's for me and they give me a $1 million guarantee that they have done it correctly and no one can steal my identity.

#29. Identity Theft Protection Using Prepaid Debit Cards

These days the credit card is as normal as the computer. In fact these days the credit card makes the computer shopping experience more useful. You can now purchase just about anything online that you can find offline and have it shipped directly to your home, usually within days, not weeks of your purchase.

Prepaid debit cards are still pretty new but the concept is catching on very quickly. In a world where identity theft is becoming very serious people are searching for a better way to secure their purchases without having to give up their identity, or rather risk identity theft.

The prepaid card is a great innovation that helps to solve this problem by allowing people to make purchases online anonymously. The card works exactly like a debit card but you are not required to attach any real information such as your name or address to the card.

Many people are purchasing these cards exclusively to shop online anonymously and to protect themselves from fraud. When your identity

is stolen you often have to go through a lot of uncomfortable hoops to restore your credit and in many cases you cannot get your money back.

With the prepaid card you can use it once and throw it away and not worry about repeat billing. Since no real information is connected to the card you don't even have to worry about shredding the card or it getting into the wrong hands because with no money on it the card is useless. You can even call and have the card number deactivated as well.

I wouldn't recommend anyone use their bank card for online purchases, there is simply too many cleaver theft potentials there. Using your bank card in stores is usually safe, but online is a whole new ball game. Prepaid cards are the greatest thing to come to the internet scene since online shopping became convenient.

You can shop with confidence and you can even track your cards spending online without having to give any information as well other than the card number. If you want to protect your spending history calling to get the number/card deactivated will delete the spending history from the site as well. The sites are secured so they are not indexed in search engines.

The beauty of the prepaid debit card is that you can purchase them just about anywhere and

activation is cheap. Many will not charge an activation fee if you put a certain amount of money on the card. At Wal-Mart you can get a free card if you cash your check there, they give you a green dot card, and you don't have to put your check on the card, you can put 20.00 on the card and cash the rest of your payroll check into cash. This is a great way to get your card without paying a fee and you can get a new one every payday.

#30. Easy Bait for ID Thieves ~ Twenty somethings

Millennials. Eighties Babies. Echo Boomers. The Connected Generation. You may think of them as tech savvy and device dependent. Identity thieves think of them as an easy victim. It's like taking candy from a baby.

Under 30? Let's see your ID.

According to a study conducted by the Federal Trade Commission, Americans age 20-29 make up 15% of identity theft complaints.

But the real threat to this age group is the severity of damage. Javelin Strategy & Research reported that 18-24 year olds spend double the amount of time on fraud resolution than other

victims. And the same age group is more at risk for debit card fraud, and more likely to have their debit card PIN stolen.

Made up of the notoriously digital generations, this age group may appear too streetwise to fall victim to identity theft. But the truth is they're constantly putting their personal information at risk.

Young and dumb? Or just naïve.

Although electronically smart, young adults are still relatively young and naïve to the risk of publicly leaking personal information. It may have something to do with the digitally connected lifestyles of Generation.

According to the same study by Javelin Strategy & Research, "In general, younger consumers tend to engage in riskier electronic behavior … With the growing use and adoption of smartphones and tablets, the risk of viruses, man in the middle attacks, and other security threats are only going to increase.

It starts with social media. Social media users with a public profile are more at risk for identity theft. And mobile devices are an additional problem—6.6% of mobile device users reported

fraud incidents.

But it also may have something to do with the turbulent lifestyle this age group often faces. Between college, different apartments, student loans, odd jobs and finding a career, the life of a twenty something is always changing—making it easier for identity thieves to make changes to records without being noticed. And without established credit and a strict budget, young adults depend on debit cards more frequently than other age groups.

Tech savvy and identity smart.

Even in an electronic world, there are a few simple precautionary measures to take to protect yourself from identity theft. Start by tightening your privacy settings on social media sites and online accounts.

1. Make sure your mobile phone has a password, and ensure that all of your passwords are complicated and secure.

2. Be sure to protect documents that contain any information regarding finances and government records.

3. Review your annual credit reports and monthly bank statements, and be careful with any documents that may contain personal information.

#31. New Account Fraud: The Cost of Remediation

Congratulations, You've Been Approved

There's a major difference in receiving a pre-approved credit card in the mail and receiving an actual credit card in the mail. The former implies a creditor wants your business. You can shred the card, remove yourself from the pre-approved credit card mailing list and get on with your life.

But receiving an actual, approved credit card in the mail is not the same thing. In fact, this could mean that an identity thief has opened credit in your name. By the time that card lands in your mailbox, it may already be maxed out and accumulating interest. Merely cutting up the card and throwing it away isn't going to fix the problem.

In the event that you do receive a credit card in the mail—say from a credit union or popular retailer—it's important to quickly jump into action. Similar to any identity theft resolution process, the steps to clean your name can cost you a lot of time and a lot of cash.

The Most Expensive Type of Fraud

When it comes to identity theft, the resolution path can be tedious and expensive no matter what type of fraud has occurred. But new account fraud—including new credit cards—is the most expensive type of identity fraud for victims to resolve.1

In a 2011 study done by Javelin Strategy & Research, victims were asked to provide a few details regarding the cost of resolution in their identity theft experiences. Here's what the numbers show:1

Average resolution time for victims of all types of identity theft: 12 hours

Average consumer cost of identity theft resolution: $354

Average resolution time in new account fraud: 26 hours

Average consumer cost of identity theft resolution in new account fraud: $1,205

The Recovery Expense Report

The victims surveyed were not given specific examples of common resolution costs or tasks, but there are several steps to resolution that are crucial—no matter what the expense. Here are a few of these steps:

(These numbers are an approximate representation. Actual costs will vary.)

Step 1: Contact the retailer where the fraudulent account was opened

If you receive a fraudulent credit card in the mail, immediately call the fraud department number on the back of the card. Have your information ready. In most cases, you will be asked to verify that the account is linked to your name and Social Security number.

After you have verified that the card is indeed fraudulent, you must specifically ask the company to start a fraud investigation. This often requires some paperwork. To speed up the process as much as possible, comply with the creditors requirements and requests.

It's also important to specifically insist that the company removes the credit application from your credit report. This type of transaction affects your credit score, so this step is critical.

Once the company has all the information they need, they will give you a fraud investigation case number. Be sure to keep this number, and any other related information, in a safe place.

Possible Costs:

- Printing costs: 4 pages for $.252

- Certified mail: $8.103

- Lost 5 hours of work: $36.254

Possible Time:

- 1-3 hours on the phone

- 60 minutes of paperwork

Step 2: File a police report with your local police department

Next, head to your local police department. You must file a report with the department located in the city where you lived when the fraud occurred.

Unfortunately, identity theft is still a widely unknown crime. Be prepared to be persistence and do some studying before you go. The Identity Theft and Assumption Deterrence Act states that as an identity theft victim, you have a right to file a police report. In many cases, there is a police report fee.

Possible Costs:

- Gas Money: $2.045

- Lost hour of work: $10.864

- Police report fee: $7.586

Possible Time:

- Driving: 30 minutes

- Filing report: 60 minutes

Step 3: Make an FTC complaint

Head to FTC.gov and fill out the complaint form. The complaint form will also serve as an Affidavit form. Keep a copy of the Affidavit in a secure place.

Possible Costs:

- Print Affidavit: 7 cents2

Possible Time:

- 15 minutes

Step 4: Put a seven-year alert on your credit reports

In order to set a seven-year credit freeze, you will need to contact each of the three credit bureaus separately and mail them the requested information. These requests usually include a copy of your Social Security number, Driver's license and proof of residence.

You will also need to send a copy of your police report and/or your Affidavit, plus any other information that the credit bureaus request. We recommend sending these confidential documents over certified mail rather than standard so that you have proof of delivery. With so much private information in one envelope, the more safety precautions you take, the better.

Possible Costs:

- 3 packets certified mail: $24.303

- Copies- 31 pages: $2.002

Possible Time:

- 60 minutes on phone

- 60 minutes for 3 packets

Step 5: Order credit reports

You will want to verify that there is no other fraudulent information on your credit reports, so you will need to request a credit report separately from each of the three bureaus. If this is the first time you are requesting reports within a year, then the service will be free. You can request your free credit reports by heading to www.AnnualCreditReport.com. Otherwise, you will have to pay full price.

Possible Costs:

- $40* to order 3 from Experian7

Possible Time:

- 15 minutes to order

- 30 minutes to review each

Step 6: Request credit reports again, 90 days after resolution

Once the investigation is over, you should receive a letter from the card issuer stating that the crime has been resolved and your identity has been

removed from the debt. Ninety days after you receive this letter, you should request your credit reports again to ensure that this information has actually been removed from your credit reports.

Possible Costs:

- $40* to order 3 from Experian7

Possible Time:

- 15 minutes to order

- 30 minutes to review each

By the end of this hypothetical situation, your total cost is $171.63 and the total time spent to resolve the issue is 9.25 hours. But if an identity thief was able to open one account, it's likely the crook may have opened another—meaning you're repeating many of these steps all over again. And these numbers only reflect some common expenses at national averages.

The Fine Print:

Identity theft is a complex crime, and a victim's

busy lifestyle only adds more obstacles. That means there's a long list of potential expenses and time-consuming tasks involved in resolving the crime. When considering an identity theft protection service, try to remember all the small costs and tasks that might add up if you don't have protection, such as:

- **Time off work**
- **Babysitters**
- **Time spent on the phone**
- **Mail expenses**
- **Driving time (post office, police department, etc.)**
- **Gas money**
- **Faxing, scanning and/or copying**
- **Additional fraudulent accounts**
- **Complications due to credit deadlines and legality**
- **Delays due to holiday hours and scheduling**

The Right Protection Offers Remediation:

An identity theft alert system is a great feature

for peace of mind. It can help consumers stay ahead of an identity thief. But what happens after the alert? What happens if an identity thief does cause damage to a member's identity?

Most identity theft services offer both an alert system and remediation services. And those remediation services may cover some or all of the above expenses, as well as facilitate the process.

Before you buy, be sure to ask what happens if you do become a victim. Comprehensive protection should come with comprehensive remediation.

#32. Social Networks

So you have a zillion "friends" on your social network. Sure about that?

More than half of U.S. adults actively use social sites such as Facebook and Twitter.1 Identity thieves are discovering the potential for financial gain by incorporating pieces of the everyday information users readily make available on these sites.

The information isn't difficult to get, either. According to a 2012 study by Javelin Strategy & Research, over 30% of social network users post their birth date. 47% share their email address and another 12% their phone number.1

By combining this information with seemingly everyday facts like birthplace, school names, locations and pet names, a smart identity thief can piece together a pretty hefty victim profile. Some of these crooks are real pros.

-More social network members creates more opportunity.-

With the tremendous growth of social networking, thieves are developing new approaches. They'll try to "friend" the target and gain more access to their lives and personal information. Another method is called "clickjacking." Thieves create malicious news and information pages where the function of a button is not what it seems. As viewers "like" and share the page with other friends, more and more victims are collected.

Spam, phishing and malware on social sites are also growing. These attacks go beyond targeting an individual's online profile and information. They aim to obtain access to the personal and financial information that is stored on the person's computer, including passwords, login

identities, banking data and other highly sensitive information.

-Safeguard yourself from friends who really aren't.-

There are ways you can protect yourself from those who pretend to be friends. First of all, consider all information, no matter how harmless it may seem, as a potential advantage for identity thieves. Use the privacy settings each social site provides to limit the amount and exposure of your personal information. Don't post birth dates, children's or pet's names, phone numbers or other specific data. Know and manage your online friends and be wary of strangers. Once they become "friends" you could inadvertently become their friendly banker.

Resources

Note: Click or Copy & Paste the Link into your browser.

Identity Theft Deterrent ~ dentity Theft Protection Without Those Monthly Fees:

Go to: http://tinyurl.com/l4z5vdo

The Busy Parents Guide To A Digital World:

(Everything You Need To Know To Keep Your Child Safe)

Go to: http://tinyurl.com/kqd8638

Wifi Sugar - Wireless Security:

(Great Software Security Product For Students, Professionals,and Travelers)

Go to: http://tinyurl.com/ny5bsoo

Don't let the crooks win and steal your identity -- protect yourself and family members.

Good Luck!

Thank You,

Terry Clark