

# Identity Theft - Nine Threats & Nine Steps To Protection

---

*Article by: Warren Franklin*

**The Bad News:** Identity theft is escalating at a torrid pace. It has become one of the country's top problems. The bad guys are finding more ways to steal YOUR identity.

**The Good News:** You can take control of the situation, become both reactive and proactive guarding yourself against identity theft.

**Identity Theft Is Spreading Faster Than The Worst Case Of The Flu!**

First, let's understand just how bad identity theft has become in this country:

- The Federal Trade Commission says that there is an underground market for credit card numbers, social security numbers and ID documents – organized gangs or web mobs use and sell these documents for as little as \$10 each. Some of these groups contain thousands of members. The amount of goods and services purchased with fraudulently obtained personal identity exceeded 52-billion dollars in 2004.
- US Department of Justice states identity theft is affecting millions of households in the U.S. each year. The cost is estimated to be six-point-four billion per year. According to the FTC, an estimated 10 million adults become victims of identity theft each year.
- The Department of Justice goes on to say that the most common misuse of identity was through credit cards, accounting for 50 percent of all identity theft. Next in line were banking and other types of accounts at 25 percent, personal information was 15 percent, and a combination of several types of identity theft was at 12 percent. The average loss for each identity theft was \$1,290.00. Two-thirds of those surveyed said the theft cost them money despite credit card coverage.
- A recent State of the Net survey by Consumer Reports which covered more than 2000 households with Internet Access projects that American consumers lost more than eight-billion dollars over the last two years to viruses, spyware and various scams. The report also shows consumers face a one-in-three chance of becoming a "cyber victim" about the same as last year. It goes on to say that consumers lost \$630 million over the past two years to e-mail scams.
- The average person today suffers through two or more "incidents" with their computer each year - the computer slows to a crawl, crashes altogether, viruses or spyware take over systems and more. It's getting worse as computers become more complex and as we do more with them.

So, Who Is At Risk For Identity Theft?

According to the Department of Justice there are three groups that are most at risk for identity theft: young adults 18 to 24, adults who earn \$75,000 per year or more and households in urban and suburban area. Interesting to note that about five percent of adults who earn \$75,000 or more a year are hit with identity theft.

The continued growth of online fraud and identity theft are putting an enormous strain on the existing infrastructure for the Internet as well as our social structure. For example, the banking community has been complacent about security upgrades required by the Federal Financial Institutions Examination Council. They report that every bank in the country has not complied with their guidelines set for now. In an article titled, "U.S. Banks Complacent Toward Identity Theft Solution," by PR Web, the single largest national security threat is a terrorist attack on our banking system. An attack aimed simultaneously at millions of user names and passwords within banks would shut down our banking system. This would instantly shut down banks worldwide. Credit/debit cards, checks, calls to the bank, would not work for at least a matter of days causing tremendous hardship and a ripple effect from no gas to "I simply have to take this baby food."

Consider for a moment some of the potential social effects from this identity theft problem. What if citizens developed a lack of confidence in our credit card and monetary system causing economic upheaval similar to what we saw in the "Great Depression?" I know this sounds radical, but what if you couldn't trust your identity to anyone anymore? What if you feared that your money, your identity was going to be stolen? It's not unthinkable that you would store your money under your mattress at home or in a safe in the closet rather than possibly losing it to identity theft. If millions of people lost faith in our monetary system and the ability to keep their identity safe and then took all of their money home where they believe it would be safe, what would happen then?

We generally can't control what happens outside of our personal environment, what happens at a bank, corporation or the government seems so far out of reach. There are, however, steps that we can take that will give us a better chance of protecting our personal information. The first step is identifying the threats and then taking steps to protect ourselves.

Below, I have identified nine identity theft threats and nine steps to protect our identity in today's society.

### Nine Threats To Your Identity

Here are nine of the most popular ways for thieves to steal your identity. Some of these are personally preventable and others are out of our control:

1. **Stolen Company Data.** Your personal information is stored on computers at stores where you shop, at your insurance company, your accountant, and more. It almost seems like a common occurrence where a company is hacked into and their customer's information is stolen. This happens so often now that the crimes are rarely reported and don't make the front page anymore.
2. **Social Engineering.** Identity Thieves are very clever. They will invent any way possible to fool you into giving your identity out. It's called social engineering because the thief uses common social situations to get the information they want. Like a seemingly innocent phone call supposedly from your credit card company asking for your personal information.
3. **Dumpster Diving.** Identity thieves get a lot of their victims' information out of garbage cans and recycle bins from old credit card statements and other personal documents thrown out carelessly.
4. **Mail Theft.** Your mail can contain valuable information: bills, banking information, credit cards, investments and more. Personal mail can often be stolen right from a mailbox.
5. **Financial Account Hijacking.** Once a thief has your personal information they can take over your personal accounts. You might not know about their activity for months.
6. **Credit Card Magnetic Strip Theft.** These clever crooks have tools to steal information off the magnetic strips on your credit card.
7. **Discarded Computers.** Your old computer really can tell stories. Even though you erased your hard drive crooks have tools to reclaim your personal information and use it against you.
8. **Spyware and Viruses on Computers.** You may not be familiar with the term 'malware.' It's a term that covers all of the hacker tools that can cause harm on your computer. These tools include spyware, keylogger tools, Trojan horses and more.
9. **E-mail and Internet Scams.** Cyber thieves are getting more and more creative using scams like Phishing, Pharming and fancy come-ons to entice you to give them your personal information.

There Are Four Ways You Can Approach Protecting Your Identity...

One way is to do nothing and hope that identity thieves don't harm you.

Second, you can be reactive. Reactive simply means that you are responding to all the material that comes your way. You are checking your credit card and bank statements to make sure nothing peculiar is on them. And if you do find something strange you contact your bank or credit card company immediately. Reactive also means that you are checking your credit report when you apply for credit or a loan.

Third, you can be proactive. A proactive approach is a more aggressive way of protecting yourself against the bad guys. You are constantly looking ahead and evaluating before giving out valuable information.

And fourth, combine reactive and proactive approaches. This is the best way to ensure you identity protection.

Nine Critical Steps To Proactively Protecting Your Identity...

Here are your 'Nine Proactive Steps To Identity Protection:'

1. Begin to operate on an "I have to know everything" approach when you give out your personal information. Only give out your personal information to people you know and trust.
2. Protect your Social Security Number, credit card and other financial information. Do not give this information out over the phone unless you initiated the call or as we stated above are talking to a trusted individual from a trusted company.
3. Cancel all of your unused accounts including banking, credit card, licenses and permits.
4. At least once a year, if not more often, update and check your credit report and Social Security Earnings and Benefits Statement to make sure everything appears as it should.
5. Protect your mail. Make sure you have a secure locked mailbox to receive all of your mail. Always mail your

payments and checks from a secure Post Office Box or from the Post Office. And, if you have a Post Office Box at the Post Office never discard your mail in a garbage can. Always bring your entire mail home.

6. Always crosscut shred all bank statements, credit card applications or information and important documents before discarding to recycle or the garbage. It is best to stir up the shredded documents to make it even harder for identity thieves to steal your information.

7. Purchase identity theft insurance. This will cover any losses incurred while recovering your lost identity once a crook has stolen it.

8. Invest in professional grade protection for your computer. The best protection available today comes from Managed Internet Security Service providers. The best security services include best-of-breed corporate grade security software for your computer, as well as unlimited service and support from trained security pros. Make sure it is the same kind of service that is used by major corporations around the world. Frankly, the over-the-counter and free security software programs available don't keep up with today's professional cyber thief. If those popular programs worked, why do we see the cyber-crime problem growing at a progressively faster pace?

A managed professional Internet security program should have the following technologies installed: A bi-directional or dual Firewall that prevents information from coming in or going out of your computer without your permission, anti-virus protection that is updated daily, and malware protection that is updated daily. Malware consists of spyware, adware, Trojan horses, keyloggers and more. It constantly changes so you will need a technology that keeps up with the professional hackers who want your identity. Your best bet is to find a professional security service that affordably manages all this for you.

9. Beware of e-mail scams like Phishing and Pharming. Phishing is an e-mail that looks like it came from a bank or business claiming you need to take care of a problem or your account will be closed down. It takes you to a page to fill out your personal information. Meanwhile, Pharming is redirecting your computer from a legitimate to a fake web site. For example, you may think that you are going to your banking site, but instead are redirected to a site that looks like your banks web site, but is hosted by an identity thief.

Identity theft continues to grow at a torrid pace. Millions of people in the United States will lose their identity to thieves in the coming year. Many of them will suffer for years trying to clean up the mess that was left behind.

The bad news is we can't control all of the identity threats we face each day. The good news is there are reactive and proactive steps we can take to protect ourselves against personal tragedy. Warren is engaged in the cause of educating and protecting people who use the Internet about the threats they face and the inadequacy of the solutions they trust, and over a two-year period has become an expert on PC Security and a passionate advocate of Internet safety. Find out more his campaign for personal and Internet security go to his web site at <http://www.completeinternetprotection.com>.