

Prevention Measures and Instructions for Identity Theft

The theft of names, addresses, social security numbers (SSN), bank account information, credit card numbers and other personal information, commonly known as identity theft is "America's fastest growing problem" according to a statement made by the Federal Bureau of Investigation. The Federal Trade Commission (FTC) estimates 10 million Americans are affected each year. With every crime, knowing how to protect yourself is vitally important to avoid becoming a victim. The following are arenas where thieves prey.

Corporate Databases and Files

Hackers regularly break security codes that protect corporate databases to gather personal information they use to take over identities. This isn't the only access weakness present. Employees have access to your information, through files, trash, and their ability to obtain information through credit reporting agencies. This may be done for their personal use or they could be conned or bribed into handing over information.

You

Constant awareness of how predators take advantage is crucial. People are mugged or pick pocketed all the time. Thieves will first follow you and easily look over your shoulder when you are using your credit or debit cards to get your pin number. Your pin can come in handy to them after they steal your cards and go crazy using them. It is frightening how easily these criminals can get at your information. They even go as far as digging in your trash for information jewel you threw out. You are not likely to hear about being robbed of your identity on the 8 o'clock news.

The Deceased

From reading the daily obituaries, a thief can take over a deceased's identity. The identity prowlers start by forwarding this person's mail which contains an overabundance of personal information, from credit card accounts to bank accounts, they in turn use.

Credit and Debit Cards

By using stolen credit or debit cards, thieves use a theft method called 'skimming' or 'eavesdropping'. According to the FTC website, "skimming occurs when an individual with [an] unauthorized radio frequency identification (RFID) reader gathers information from a RFID chip [located on credit and ATM cards] without the cardholder's knowledge. Eavesdropping occurs when an unauthorized individual intercepts data as it is read by an authorized RFID reader." The person swiping your cards could be stealing your information. This criminal skill can be done to the deceased and living.

Faux E-mails & Websites

Very sophisticated thieves, if they can be called that, send out e-mails under the names of legitimate websites asking for updates on information but once you hit the link the e-mails direct you to very professionally-made, fake websites. They appear to be identical to the real site you are used to. The one thing lacking is a secure, encryption system. They will ask you to log on with your user name and password which they will use later on the real website. This type of identity theft is called 'phishing' because thieves are 'fishing' for your information, the most publicized method used in identity theft.

What's Next?

If you are already a victim, the novice criminal will just rack up your credit cards, open up a new cell phone account and possibly get some new credit cards in your name, while the professional criminal will wreak havoc. They literally take on your identity; they take your name becoming you; and they get drivers licenses as you, but with their picture. They will use their newly acquired identity to get loans, open bank accounts and take out mortgages. When they, or should I say, you don't pay for these, they claim bankruptcy which quite obviously damages your credit. If arrested for any crimes committed, criminals will use your name then, too. So now, you have a criminal record on top of everything else.

An Ounce of Prevention Goes a Long Way

It is common knowledge today that a well-balanced diet and exercise program can prevent diseases like cancer, diabetes, and high blood pressure, just to name a few. Prevention is also key to protecting your identity. Putting into practice the following suggestions will lower your chances of becoming a victim.

Social Security Number - SSN

Take a moment and think about all the instances you have provided your social security number (SSN). Was it necessary? The "do's" and "don'ts" for this vital personal identification number are the following:

Do use alternative identification like a drivers license when possible

Do question the necessity of handing out your SSN on medical forms, job or college applications and for fishing or hunting licenses. There is no telling how they file this information and the amount of people who will readily have access. After inputting the information on the form into their database, how do they destroy the form or do they just throw it out for anyone to pick it out of their trash?

Your SSN is a critical part of your identity that serves criminals in a multitude of instances. Don't be embarrassed to first ask before divulging this information, your identity might depend on it and there is nothing embarrassing about that.

Don't write your SSN on any type of ID, credit card and especially, don't print it on your checks.

Don't ever carry your SSN card with you in your purse or wallet.

Mail

Most mailboxes are not locked and are an easily accessible source of information. Pre-approved credit card offers along with other offers that could be filled out with your information come in the daily mail. The Federal Trade Commission suggests calling 888-5OPT-OUT or logging on to <https://optoutprescreen.com>, operated by the major credit reporting agencies; registration will prevent offers for prescreened credit card and insurance. They also give you an option of opting out for five years or permanently. They do ask for personal information, including your home telephone number, name, SSN, and date of birth but this is a secure site that keeps this information confidential and uses it to process your request. If offers continue coming in the mail, shred them. Purchase a cross cut shredder and shred any mail with identifying information. Done daily, it's not that hard to do. When in doubt, shred it.

Do you put up the flag on your mailbox to let the mailman know you have outgoing mail? Who else do you think this red flag alerts? You guessed it.

Are you in the practice of writing your credit card number on your monthly payment checks? If so, stop. Write only the last four digits of your account and definitely, do not write your social on it. Another precautionary suggestion, deliver any outgoing mail to the post office and completely eliminate this temptation. While you are there, suspend your mail delivery if you plan on going on vacation. Bulging mailboxes are equally tempting.

Trash

The above suggestion about shredding might not have been sufficiently clear on its importance. Shred any credit card offers, card or bank statements, receipts, bills, and all mail that has your name on it. Don't give criminals the opportunity. Picking up the trash before the sanitation trucks drive by, they can go home and rummage through it in their garage. This is not being obsessive, it is common sense. Thinking like a criminal and not giving their menacing tactics anything to look at. Shred, shred, and shred some more! Those old credit cards you had but aren't using any more, don't cut them up with your scissors, shred these too. Pulverize them! Are you getting the point? Shred everything before putting it in the garbage. Another option is to lock up personal and financial files in a safe or safety deposit box.

Telephone

Telemarketers can represent legitimate companies but a tell-tale sign you're being sucked into a scam is when the offer is too good to be true and the caller starts asking for your social, credit card number, and other personal information. Don't be fooled if the caller tells you they are calling from your bank, doctor's office, laboratory or other familiar businesses you deal with. Before giving them any information, tell them you will call them right back with the information and use the phone number you have not the one they give you to call back. Contact your bank or doctor's office to verify the call. More often than not, it's a hoax.

To avoid these calls all together, register with the FTC's "National Do Not Call Registry." If they continue to call, tell them you're on the do not call list and request they add you to their list as well. Hanging up is alright, too. Continued calls for the same company or organization, as well as fraudulent calls should also be reported to the FTC. This activity is a federal offense and companies can be fined for it.

Wallet

Three precautions come to mind when protecting your wallet:

1. Write 'photo ID required' in the signature box of your credit and debit cards. Do not sign them.
2. Today, some banks issue cards with your picture on the front. These are a favorite and an attractive incentive for opening up an account with them. You're reducing risks by putting a picture that businesses can use to verify your identity.
3. Take everything out of your wallet that you normally carry with you. Photocopy or scan everything including the front and back of cards. If you are ever mugged or pick pocketed, you can provide authorities with visible proof of what was stolen and you'll have companies' phone numbers to call immediately and notify them of your loss. It should go without saying but will do so; photocopies should not be kept in the wallet but in your safe at home.

Personal Computer (PC)

Computers should be protected with a password, although this is not fool proof and professional criminals find their way around them. For a common thief, the trouble required to figure out the password will be a deterrent. Change the password to your computer often, along with passwords to sites you frequent. Use the computer to look up your name and the last four digits of your social on the World Wide Web. Thieves do slip up from time to time and you may catch them on the internet.

Deceased Relatives

Once a loved one passes away, you may want hire a lawyer to help you, identify any financial, credit card, insurance and/or loan companies the deceased might have had accounts open with or had done business with. Joint accounts should also have the deceased's name removed. Provide all the above institutions with a copy of the death certificate, request the accounts to be closed and that an official letter confirming this action be mailed to you.

The major credit reporting agencies (i.e. TransUnion, Experian, and Equifax) should also be notified. If an [identity thief](#) tries to use the deceased's credit, the agencies will realize there is a 'deceased alert' and will tell the company that the person is dead and cannot be issued credit.

Credit Report

Annually check your credit report from the credit reporting agencies, noted previously. Look for any credit cards you do not own, loans you have not taken out, and any other suspicious activity. Report anything unusual, or if you think you have been robbed of your personal information, file a report with authorities immediately. You should bring along any proof you have found to substantiate your claim. Complaints can also be reported to the FTC by calling 1-877-IDTHEFT.

Conclusion

In a nut shell, becoming a victim of this crime encompasses the loss of money, it ruins your credit, criminal record, your name, and will be emotionally devastating. Keeping your guard up and staying current with new techniques being used in the identity theft world is an advantage you are giving yourself. The FTC website <http://www.ftc.gov> provides consumers, like you, many tools, tips, and breaking news. Add them to your 'favorites' and visit their site regularly.

About the Author

In times like these it is easy to see why so many people like yourself are interested in [identity theft protection statistics](#). Visit us at <http://www.everlife.com/identity-theft.php>.

Source: <http://uniquefinancialarticles.com>