

Identity Theft

Protecting Sensitive Information

- **40 Precautions for Preventing Identity Theft**
 1. Never give out your social security number unless it is absolutely necessary for what you need to do.
 2. Even if you have to give it out, make sure you know for sure who you are giving it to. Being comfortable with them is not enough. Know the other party and what they do, how they will use that number and where their privacy policy is located.
 3. Do not carry your social security card anywhere!
 4. Get a paper shredder so no one can piece together important information (at the very least, rip up the documents yourself)
 5. Protect those PIN numbers - Cover the number pad when you are entering pins at the ATM machine and never tell anyone about them. Also, never use something like 1234 as your pin please!
 6. Pay a little more for an unlisted number - Again, less telemarketers mean less chances that you can become a target.
 7. Try to separate your personal information as much as possible - Don't write your SSN on your checks or keeping your driver licenses with your SSN card. If something is lost, at least the crooks only have one piece of information and not everything about you.
 8. Don't Trust Anyone Over the Phone - Never give anything out over the phone. It's just too dangerous.
 9. Do not keep any sensitive information in your car - Credit cards, statements, checks are a nono.
 10. Buy a safe - Better yet, get a safety deposit box at the bank where you can put important documents.
 11. Educate Others - If everyone teaches others about protections, there will be less identity thefts and less people who will try to do this because it's not as lucrative!
 12. Be Alert - Think about how your identity can be stolen whenever you are dealing with your own sensitive information.
 13. Be Clam and Patient - Don't do something with checks, credit cards, SSN numbers etc when you are in a rush!
 14. Blank Spaces - Always draw a line on blank spaces: On credit card receipts, always write your amount with a \$ symbol followed immediately with the numbers. On checks, always draw a line after your write the amount in English (or in numbers).

Credit Report and Monitoring

15. Sign up with a credit monitoring company like Equifax Credit Watch.

16. Freezing Your Credit - You can call the credit report agencies to freeze your credit so no one can ever apply for a credit card or get a loan under your name until you unfreeze it. It will cost money but the piece of mind might be worth it.
17. Get free credit reports so you can check them (remember that if you don't cancel your membership, they will charge you a monthly fee)

Knows Your Credit Cards

18. Always know how many credit cards you have. While most people believe that cutting up used credit cards and not canceling them is better for your credit score, you run the danger of having others make fake cards as you lose track of how many accounts you have opened.
19. Credit Card Receipts - Never leave them behind even if it doesn't have the full credit card number. Gas stations, restaurants are the two places I see receipts all the time.
20. Instead of signing the back of the credit card, write "Check ID".
21. If your credit card company offers it, opt for the card that has your photo on it.
22. Create a list of phone numbers and credit cards that you have (it's not absolutely crucial that you record the full credit card numbers on it but if you do, remember to keep it in a secure place). In case your wallet is stolen, you can quickly call all card companies to cancel those cards.
23. One Off Credit Card Numbers - Some credit card companies will generate an "one-time-use" number for you to use online. Seriously consider using these.

Computers and the Internet

24. Only make online purchases through trusted websites. Stuff like the Trust-e symbol, better business bureau stamp are a must.
25. Install anti-virus or anti-spyware on your computer and never open links through an email unless you are absolutely sure that it's safe. For now, you can also use a Mac instead (until macs get popular enough that crooks start targeting it as well)
26. Monitor all your accounts online - Check your accounts regularly now that it's so convenient to monitor them online. Make sure there's nothing suspicious going on.
27. Passwords - Never save your passwords just for the convenience. Typing it out doesn't take that much time! Also, the more complicated it is, the better. Remember to also use capitals, letters, symbols and letters.
28. More about Passwords - Change them regularly.
29. Security tokens - Some banks are starting to offer those security tokens that change numbers every few seconds as an added security over your password when logging onto your online account. Take advantage if yours offer one.
30. Don't log onto accounts using a public computers - You don't need the possible hassle of forgetting to log out.

Secure Your Mail and Mailboxes

31. Turn your checks backwards when mailing them so the information is facing inwards
32. Better yet, get non-see through envelopes so no one knows what's inside.
33. Limit the credit cards you have. You don't need an army of credit to buy your groceries.
34. Never leave bills in your mailbox for the mailman. Deliver it to the post office.
35. When you move, contact all credit card, creditors, and IRS immediately of the address change.
36. Go to opt-out prescreen and take yourself off the mailing list that credit card companies use to send out those "pre-approved junk mail".
37. Sign up for electronic delivery of your bills - No more mail, no more possible lost mail.
38. If you don't opt for electronic bills, make sure you are getting all your bills. A missing bill should sound off an alarm.
39. Consider a P.O. box for your mail if the mailbox in your neighbor aren't safe enough.
40. Take your mail as soon as your mailman delivers it. If you pay attention, you will realize that he/she comes around the same time every business day.

These aren't so hard to implement right? If you do all of the above, you will greatly reduce the chances of becoming an identity fraud victim. Start now and practice fraud prevention!

How to Prevent Identity Theft

1. Step 1

Avoid writing personal checks to people you don't know. Give a money order, a bank draft or cash instead. Nowadays it is very easy to pull funds from anyone's bank account via online rout. Even if you never signed up for an online banking, anybody can pull funds from your account through the internet. All one needs is your bank account number and the bank routing number plus your name; all this information is written on the personal checks that you write.

2. Step 2

Before dumping your bank statements to garbage know this: hackers don't have access to your office or bed rooms, they search your trash cans for vital information and many times they are successful. So buy a shredder. Destroy fully your statements before putting them in a trash cans.

3. Step 3

Sign up for 'online statements only'. Most of banks mail bank statements via a regular mail. There is no guarantee it would not be opened by another person. it has most of your banking information.

4. Step 4

We often receive credit card promotional checks in mail. These are the easiest checks to cash. They don't even need your signatures. Remember, unlike checking accounts, majority of the

creditors do not have your signature on files for comparison. Call your creditors to stop sending such checks to you.

5. Step 5

Destroy your 'expired' credit and debit cards. Know that the creditors do not change the number on your credit cards when they mail out the new ones. The only thing that changes is the expiration date. No doubt an expired card cannot complete the transaction if swiped, but, to make an online purchase all you need is the card number and the name of the card holder. Many sites neither ask for the CV code (found at the back of the card) nor are they very particular about the accuracy of the expiration date. Therefore, all the information required to make an online purchase is present on your expired cards.

6. Step 6

Be sure to sign the back of your credit or debit cards. It's a good idea to put a piece of transparent tape over the signature so that it cannot be tampered. A store cashier sometimes compares the signature of the holder with the one present on the signature panel of the card, especially when a big purchase is made. If you have not signed the back of your card you are risking an unauthorized use. Anyone who possesses your card can misuse it because there is no signature to compare.

7. Step 7

Pre-approved credit offer letters are as dangerous as the bank and credit card statements. Its easy for an identity thief to draw credit in your name using those pre-approved offers. Such offer letters should be handled in the same way as your other financial statements. Also, I recommend to call the toll free number printed on such offer letters to opt out of receiving them in future.

8. Step 8

Avoid using public computers, such as in public libraries, work places, 'hotspots', for accessing your bank accounts, credit cards, applying for credit cards online. User IDs and pass words are stored in computers as cookies. They are easily accessible to hackers. Even if you do use public computers make sure you clear the stored cookies after you logout. Here is how you can do it: go to 'tools' tab. click on 'internet options' then from the window that will open up click 'delete cookies', then, 'delete files' (make sure you check 'delete all off-line content' in the prompt window) and finally 'delete history'. However, many public computers have disabled access to 'internet options' unless you are logged in as administrator. So it is advisable to check if you would be able to access internet options in tools menu prior to logging in to your bank accounts at public computers.

9. Step 9

Shut of your home computer when not in use. At least put it to 'sleep' mode. Open connected computer is an open book for hackers in cyber space to access. They can retrieve all your cookies (pass words, user ids etc). Many times while surfing internet small windows pop up prompting you to either cancel or OK an action. Many times even if you click 'cancel' some small software gets installed into your computer that hooks a hacker sitting elsewhere to your computer. He gets instant access to your files, pass words etc. Check your computer frequently for such installed programs. Here is how to do it: go to 'control panel'. Click on 'install-uninstall programs' from the window that opens up you will be able to see list of all the programs that are installed in your computer. If you do not recognize any program it is safe to uninstall it by clicking on the program once and then clicking on the 'uninstall' tab.

Other Links:

- [Preventing Identify Theft a Guide for Consumers \(PDF\)](#)
- [Strategies for Preventing Identity Theft](#) (from [About.com](#))
- [Fight Identity Theft](#)