

## Top Tips to Protect Yourself Against Frauds and Scams, Identity Theft and Reduce Spam Email

What can you do to defend yourself from scams, frauds and identity theft? Whether you think you have been the victim of a fraud or scam or want to be proactive in protecting yourself, here is a list of specific and simple actions that you can take, some just once, to protect yourself and your family! We have ranked them in order that you should take them:

1. **Don't use or carry a checkbook.** Pay by cash or credit card. Paying your bills through your bank or credit union's online bill paying service (which is usually free) is much safer than mailing a check.
2. **Buy and use a paper shredder.** Shred any documents that have your social security number or other financial information, such as your bank account numbers, credit card numbers etc. Identity thieves actually go through homeowner's trash to obtain personal information. If you don't have a shredder, burn these documents completely in the fireplace.
3. **Freeze your credit!** It prevents scammers from opening unauthorized accounts in your name. Even if your state is one of the few that doesn't allow a freeze, thanks to pressure from consumer advocacy groups, you can still freeze your files at the three major credit bureaus.
4. **Sign up on the [Do-Not-Call List](#)**
5. **[Sign up to block credit card offers](#)** from arriving in your mailbox.
6. **Don't carry your Social Security card with you.** When you renew your driver's license, make sure the DMV does not use your Social Security number as your driver's license number.
7. **Use a separate email address when you post messages to any public forum,** such as newsgroups and mailing lists. Free email accounts from [Yahoo](#) and [Hotmail](#) are perfect for this. Never use your personal email address for this purpose: you will be flooded with spam. You can periodically check this email account to see what's spam and what isn't. A bonus is that Yahoo's spam blocker is better than those from most ISP's! And your main personal email address won't be as clogged with spam. Some ISP's, like AOL and BellSouth.net give you multiple email accounts free with your paid service.
8. **Don't give out any financial information,** such as checking account and credit card numbers; and especially your social Security number; on the phone or online, unless you initiate the call and know the person or organization you're dealing with. Don't give that information to any stranger. In general, it is only required for medical providers, banks, mortgages and credit card companies.
9. **Don't fill out the "win a vacation"** and other promotions you see in stores and shopping malls. That will just get you on a junk mailing list and guarantee calls from persistent, high-pressure salesmen.
10. **Don't pre-print your driver's license, telephone or Social Security numbers on your checks.** And in states that want to use your social security number as your driver's license number, insist on another method - most allow it.
11. **Report lost or stolen checks immediately.** The bank can block payment on the check numbers that are missing. Also, review new checks you receive, to make sure none has been stolen in transit.
12. **Store new and cancelled checks, credit card statements, medical bills, anything with confidential information, in a safe place and shred them when you are done with them.**
13. **Guard your Personal Identification Numbers (PINs)** for your ATM and credit cards, and don't write on or keep your PINs with your cards. You should also guard your ATM and credit card receipts. Thieves can use them to access your accounts.

14. **Be creative in selecting Personal Identification Numbers** for your ATM and credit cards, and passwords that enable you to access other accounts. Don't use birth dates, part of your Social Security Number or driver's license number, address, or children's or spouse's names. **Remember:** If someone has stolen your identity, he or she probably has some or all of this information.

15. Use a good anti-virus software, anti-adware software and a hardware firewall on your computer, and keep them up to date. You need all three. Almost all modern Routers (Dlink, LinkSys, NetGear, Buffalo, Airlink, etc.) have a hardware firewall built in. See the left side of this page for the current recommendation for ant-virus / anti-malware programs.

16. **Don't put outgoing mail in or on your mailbox.** Drop it into a secure, official Postal Service collection box. Thieves may use your mail to steal your identity.

17. **If regular bills fail to reach you, call the company to find out why.** Someone may have filed a false change-of-address notice to divert your information to his or her address.

18. **If your bills include suspicious charges, don't ignore them.** Instead, investigate immediately to head off any possible fraud before it occurs.

19. **Check your credit report regularly.** Federal law allows you to obtain one from credit report from each of the 3 major credit reporting agencies per year.

20. There are [services online](#), some free, such as [SneakMail](#) that provide you with disposable addresses that can be deleted if they begin to receive spam messages. The disposable email addresses forwards email to a real email address of yours, but the sender can not see this. If you create a unique address for each email newsletter or forum you subscribe to you can discard the address if it gets too much spam and just start using another email address.

21. **NEVER buy anything from a company that sends you spam.** Don't even visit their sites or ask for more information. It is like feeding a stray cat. Give it one morsel of food, and it will be there all the time (and that may be fine with cats, but NO one wants spammers at the doorstep!). Remember, since they send out millions of spam emails, they only need a tiny fraction of responses to be profitable. And if that doesn't convince you, consider this: the vast majority of spam "offers" are in fact scams!

22. **Set up filters in your email program.** Outlook does this quite easily. When you open an email and realize that it is spam, just click on Actions then Create Rule, then select an appropriate action, such as "from" then click "Move e-mail to folder" and select the "Deleted Items" folder. That's it! You'll never receive email from that particular address or subject again!

23. **If you have a website, do not post your address in the HTML "mail-to" format,** otherwise you will be spammed, since address-harvesting spiders (programs) extract your email address from the website and add it to the spammer's lists. Instead use feedback forms through PHP, ASP, or JSP that hide the email address, OR post the email address as a GIF (image file).

24. **Finally, if it seems too good to be true... IT IS!** No one is going to send you a pile of money from a dead Nigerian president, no lottery is going to make you a winner from a "randomly selected from a database of email addresses". Multi-level marketing IS A SCAM, ALL psychics are nothing more than conmen, and you can not make big money from "passive residual income in a few hours of your spare time each day". And there is no Easter Bunny.