

We've all seen the commercials featuring stolen identities, and been barraged with e-mails from "government officials" needing access to our checking account numbers so they can deposit millions of dollars. With so many transactions taking place online, it's inevitable that some tech-savvy hackers will try to get our information. A few precautionary measures—both online and otherwise—can help you keep these swindlers from getting you.

Ten Tips to Prevent Identity Theft

- 1. Watch for shoulder-surfers.** When entering a PIN number or a credit card number in an ATM machine, at a phone booth, or even on a computer at work, be aware of who is nearby and make sure nobody is peering over your shoulder to make a note of the keys you're pressing.
- 2. Require photo ID verification.** Rather than signing the backs of your credit cards, you can write "See Photo ID."
- 3. Shred everything.** One of the ways that would-be identity thieves acquire information is through "dumpster-diving," a.k.a. trash-picking. If you are throwing out bills and credit card statements, old credit card or ATM receipts, medical statements or even junk-mail solicitations for credit cards and mortgages, you may be leaving too much information lying about. Buy a personal shredder and shred all papers with personally identifiable information (PII) on them before disposing of them.
- 4. Destroy digital data.** When you sell, trade or otherwise dispose of a computer system, or a hard drive, or even a recordable CD, DVD or backup tape, you need to take extra steps to ensure the data is completely, utterly and irrevocably destroyed. Simply deleting the data or reformatting the hard drive is nowhere near enough. Anyone with a little tech skill can undelete files or recover data from a formatted drive. Use a product like ShredXP to make sure that data on hard drives is completely destroyed. For CD, DVD or tape media you should physically destroy it by breaking or shattering it before disposing of it. There are shredders designed specifically to shred CD/DVD media.
- 5. Be diligent about checking statements.** This actually has two benefits. First, if you are diligent about checking your bank and credit statements each month, you will be aware if one of them doesn't arrive and that can alert you that perhaps someone stole it from your mailbox or while it was in transit. Second, you can ensure that the charges, purchases or other entries on the statement are legitimate and match up with your records so that you can quickly identify and address any suspicious activity.
- 6. Pay your bills at the post office.** Never leave your paid bills in your mailbox to be sent out. A thief who raids your mailbox would be able to acquire a slew of critical information in one envelope—your name, address, credit account number, your bank information including the



routing number and account number from the bottom of the check, and a copy of your signature from your check for forgery purposes just for starters.

7. **Limit the information on your checks.** It may be convenient to have your driver's license number or social security number imprinted on your personal checks to save some time when you write one, but if it falls into the wrong hands it reveals too much information.
8. **Analyze your credit report annually.** This has always been good advice, but it used to cost money, or you had to first be rejected from receiving credit so that you could get a free copy. Now it is possible to get a free look at your credit report once per year. The big three credit reporting agencies (Equifax, Experian and TransUnion) joined forces to provide free credit reports to consumers. The web site, **www.annualcreditreport.com**, is currently available for the Western and Midwestern states, with the Southern and Eastern states being rolled out later this year. You should review it to make sure the information on it is accurate and also make sure that there aren't any accounts on there that you aren't aware of or any other suspicious entries or activity.
9. **Protect your Social Security number.** It is often suggested that you do not carry your Social Security in your wallet with your driver's license and other identification. Knowing your full name, address and full Social Security Number, or even the last four digits in many cases, can let a thief assume your identity. You should never use your Social Security Number as any part of a username or password that you establish and you should never divulge it to telephone solicitors or in response to spam or phishing scam emails either.
10. **Caveat Emptor.** You can feel relatively secure doing business online with Amazon.com or BestBuy.com or any web site affiliated with well-known, national or global merchants. But, if you are buying something online you need to have some level of trust that the company you are doing business with is legitimate and that they take the security of your personal information as seriously as you do. When you do make online purchases, read the company's online privacy policy first to ensure you agree with it and make sure you are on a secure or encrypted website (symbolized by a small padlock at the bottom right of the screen in Internet Explorer).



Source: Tony Bradley at About.com

This information is brought to you by **FedSource** & GuidanceResources®. Our Guidance Consultants can assist you with behavioral health concerns at: **888.290.4EAP**

TDD: 800.697.0353

Online: **www.guidanceresources.com**

Enter your agency ID: **Fedsource**