COMMONd
We help organizations do more for less

Identity Protection 100

Every 79 seconds there is another victim of identity theft. Phishing, on-line financial fraud, and dumpster diving are increasingly becoming compelling drivers for us to protect our identity.

If you are an ID thief's mark, you will likely face the risk of lost money and frustration as you work to clean up the mess.

The best protection is to have common sense and to pay attention; bad guys are indeed watching you. Here are some ways to safeguard your identity:

Low Tech High Touch

1. Buy a shredder and use it. Shred everything: old bank statements, medical statements, everyday bills, and pre-approved credit card offers. Shred any document that has personal financial information on it.

2. Monitor your credit card statements carefully and cancel any unused ones.

3. Know your credit score and get a credit report once a year. Clean up any errors.

4. Protect your Social Security number. Only give your Social Security number when absolutely necessary. Avoid using it as your account number or PIN number whenever possible. If any one demands it, ask for an alternate number. If at all possible, do not have it published on your driver's license.

5. Do not carry your Social Security card or your Social Security number in your wallet.

6. Keep an inventory and list all of your credit cards, loans, account numbers and expiration dates in a safe place so you can notify creditors in case of changes, theft or loss.

7. Never give a credit card number or loan account information over the phone unless you initiated the call.

8. Watch for "shoulder surfing." Take care when using ATM machines to shield the keyboard from view when you enter your PIN. Someone could look over your shoulder, memorize your PIN, and use it to gain access to your information later.

9. Ask questions whenever you are asked for personal information that seems inappropriate for the transaction. Ask how the information will be used and if it will be shared. Ask how it will be protected. Explain that you're concerned about identity theft. If you are not satisfied with the answers, consider going elsewhere.
10. Stop pre-approved credit offers as much as possible. They make a tempting target for identity thieves who steal your mail. Have your name removed from credit bureau marketing lists. Call toll-free 888-5OPTOUT (888-567-8688).

High Tech High Touch

1. Click carefully and look for opportunities to opt out of information sharing. Only enter personal information on secure Web pages with “https” in the address bar and a padlock symbol at the bottom of the browser window. These are signs that your information will be encrypted or scrambled.

2. If you're shopping with an online merchant, look for the Trust-e symbol or a Better Business Bureau online seal.

3. Only shop on web sites that offer a privacy policy. Know how your personal information will be handled. Print out privacy policies, warranties, price guarantees and other important information.

4. Control your personal financial information. California law requires your bank and other financial services companies to get your permission before sharing your personal financial information with outside companies. You also have the right to limit some sharing of your personal information with the company that you are doing business with.

5. Do not use public computers for sensitive transactions and information. Be aware of this if you are traveling. For instance: hotel, library or computer at work.

6. Do not open links in emails. Hackers frequently try to get information from individuals by sending emails asking for verification of account information. These deceptive emails may say that your bank account has been closed due to fraudulent activity or that it needs to be verified. If you ever receive an email of this nature, do not open the attached files. And call your financial institution immediately.

7. Whenever you’re not using the Internet, disconnect your Internet access.

8. Make sure any online credit card charges are handled through a secure site or in an encrypted mode.

9. Update your online accounts. This is perhaps the easiest precaution! Change your password at least every six months. Choose passwords that are not obvious and that would be difficult to guess. To strengthen security, choose a password consisting of both alphabetic and numeric characters. And remember – never share your password with anyone else.

10. Install a firewall for your personal computer. This is your computer’s first line of defense. It will not completely protect your machine from hackers and intruders, but it will minimize it.

11. Use anti-virus software with spyware, spam and phishing protection. It you have multiple computers networked in your home, find one with network mapping utilities.

12. Update your computer as often as possible—at least once each week.