

The Federal Trade Commission estimates that nine million Americans become victims of identity theft annually. Not only does identity theft cost victims hundreds of dollars but credit reports are inevitably damaged causing an array of consequences from lost job opportunities to denied loan applications. And identity theft can sneak up on you—you may not even know someone has gotten hold of your credit card number until you receive a call from a debt collector (www.ftc.gov)

There are many ways for a thief to come after your personal information:

Dumpster Diving Identity thieves will rummage through your garbage or recycling bins in search of pre-approved credit card forms, bills or any other papers with personal information.

Phishing E-mails from scammers that appear legitimate (for example, the e-mail may seem to be from your insurance company) that try and get you to “verify account information.”

Pretexting Very similar to phishing, except the attempted identity theft is via phone calls instead of e-mail. Again, the caller will impersonate a legitimate company in order to persuade you to give out personal information.

Changing Your Address Re-directing your billing statements to another address is as easy as filling out a change of address form.

(Retrieved from www.ftc.gov)

Two of the simplest things you can do to protect yourself against ID theft is to buy a shredder and remove your Social Security Card from your wallet.

Shredding *all* documents that have personal information on them, including mail and bills, protects you against someone snooping through your trash can or recycling bin, and keeping your Social Security Card in a safe, secure place is a preventative measure in case your wallet or purse is stolen.

And don't forget your Medicare card—that also has your SSN. Only carry your Medicare card with you if you absolutely need it.

Follow These Tips to Protect Yourself from Identity Theft:

- **Don't toss your outdated computer without destroying the hard-drive.** Even if you've erased the drive, computer-savvy people can still retrieve information. You will need to physically destroy the hard-drive—think sledgehammer.
- **Don't click on “Remember Me” prompts** that enable you to automatically log-on the next time you visit a website. Computer hackers are able to obtain that information and gain access to your e-mail, online bank account, etc.
- **Don't access sensitive information at a library, Starbucks WiFi spot** or any other public computer or wireless network. Just like you wouldn't want someone to peep over your shoulder to see your pin number at an ATM, logging on to Panera's wireless network to pay your bills puts you at risk. (If you have wireless set up at home, make sure it is protected with a password.)

- **If your wallet gets stolen** would you be able to remember what all was in it? Make photocopies of your driver's license, credit cards and insurance cards.
- **Review all financial statements and bills**—from your credit card statements to your Social Security—for missing bills, for charges you don't recognize and for errors.
- **Always be skeptical.** There are a lot of ways for scams and frauds to find their way into your home whether via phone, e-mail or your mailbox. Before providing requested information, always verify that businesses, charities and others who contact you are who they say they are by checking with the company using a phone number you know is valid.

(Retrieved from www.ncscam.gov and www.fightidentitytheft.com)

For more information on Identity Theft and how to protect yourself, check out:

www.ftc.gov

www.idtheftcenter.org

www.ssa.gov

www.identitytheft.com

www.privacyrights.org/identity