

## Recognize and Protect Yourself from Identity Theft

Stephanie Obodda - 2016-07-11 - Comments (0) - Identity Theft

The following tips can help lower your risk of becoming a victim of identity theft.

- **Protect your Social Security number.** Don't carry your Social Security card or other cards that show your SSN. Read, [Identity Theft and Your Social Security Number](#).
- **Use caution when giving out your personal information.** Scam artists "phish" for victims by pretending to be banks, stores or government agencies. They do this over the phone, in e-mails and in postal mail.
- **Treat your trash carefully.** Shred or destroy papers containing your personal information including credit card offers and "convenience checks" that you don't use.
- **Protect your postal mail.** Retrieve mail promptly. Discontinue delivery while out of town.
- **Check your bills and bank statements.** Open your credit card bills and bank statements right away. Check carefully for any unauthorized charges or withdrawals and report them immediately. Call if bills don't arrive on time. It may mean that someone has changed contact information to hide fraudulent charges.
- **Check your credit reports.** Review your credit report at least once a year. Check for changed addresses and fraudulent charges. To order your free annual credit reports, visit <http://www.annualcreditreport.com> for details.
- **Stop pre-approved credit offers.** Pre-approved credit card offers are a target for identity thieves who steal your mail. Have your name removed from credit bureau marketing lists. **Call toll-free 888-50P-TOUT (888-567-8688).**
- **Ask questions.** 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. If you're not satisfied with the answers, don't give your personal information.
- **Protect your computer.** Protect personal information on your computer by following good security practices.
  - Use strong, non-easily guessed [passwords](#).
  - Use firewall, anti-malware software that you update regularly, such as [Forefront Endpoint Protection](#) (Windows) and Sophos for Macs ([on-campus/VPN version](#) | [personally-owned computers](#))
  - Download software only from sites you know and trust and only after reading all the terms and conditions.

- Don't click on links in pop-up windows or in spam e-mail.
- **Use caution on the Web.** When shopping online, check out a Web site before entering your credit card number or other personal information. Read the privacy policy and take opportunities to opt out of information sharing. Only enter personal information on secure Web pages that encrypt your data in transit. You can often tell if a page is secure if "**https**" is in URL or if there is a padlock icon on the browser window.