

### Identity Theft

1. Monitor your credit cards / bank accounts daily (or at least weekly); subscribe to alerts
2. Limit the number of credit cards you use
3. Use a separate credit card for on-line shopping, Ebay, Paypal, etc.
4. Use credit cards, not debit cards
5. Make copies of credit cards, etc. in your wallet; don't carry Social Security Card
6. Stop pre-approved credit card offers: [optoutprescreen.com](http://optoutprescreen.com)
7. Protect your social security number. Do not give out your social security number if you don't have to.
8. Pick up mail every day
9. Shred anything with you name on it
10. If you have or suspect identity theft, institute a 90-day fraud alert through one of the credit reporting agencies (Experian, Transunion, or Equifax)
11. Monitor your credit by requesting your free annual credit report
12. If you are a victim of identity theft, file a police report
13. If you are a victim of identity theft, go to the Federal Trade Commission's web site for free assistance: [IdentityTheft.gov](http://IdentityTheft.gov)
14. Other considerations:
  - Child ID theft
  - Deceased ID theft
  - Medical ID theft
  - Tax ID theft

### Computer Hacking / Identity Theft

1. Never email anything containing personal information
2. Do not click on links in emails – even surveys
3. Do not make transactions from a public network
4. Have good anti-virus software on home computer
5. Protect passwords; do not have passwords that tie back to you (birthdates, addresses, etc).
6. Make sure you are doing on-line transactions with a secure browser: <https://>
7. If using Internet Explorer, consider removing add-ins
8. Limit social media sharing

### Personal Safety

1. Do not open your front door unless you know who it is
2. Secure your billfold / purse
3. Maintain situational awareness