

## Protect your Social Security number (SSN).

- Don't carry your Social Security card in your wallet.
- Avoid carrying cards with your SSN, particularly health insurance cards, unless you need them to receive care.
- Request that your driver's license number is not the same as your Social Security number.
- Never give out your SSN, credit card number, or other personal information over the phone, unless you have a trusted business relationship with the organization and initiated the call using a verified phone number.
- Avoid including your SSN on job applications.
- Provide your SSN only when absolutely necessary—for tax forms, employment, student records, stock and property transactions, etc.
- If your financial institution attempts to use your SSN as an account number, ask them to change it immediately.
- If a government agency requests your SSN, look for a Privacy Act notice. This will state whether a SSN is required, how it will be used, how it is protected, and what happens if you don't provide it.

## Protect what's in your wallet, pocket or purse.

- Never leave your wallet or purse in your car, not even in the trunk.
- Whenever possible, avoid carrying these items with you: birth certificate; passport; military identification card; driver's license or insurance card with SSN on it; banking information (PINs, logins, passwords, or account numbers); paychecks; pay stubs; and deposit slips.

## Protect your mail.

- Use either a secure locking mailbox or a post office box.
- Never place outbound mail (at home or work) in an open, unlocked mailbox.
- Never leave mail in your car.
- Investigate immediately if expected statements or bills from your financial institutions do not arrive on time.
- Be especially vigilant during January and April when tax documents are sent out—they're favorite targets for identity thieves.
- During extended absences, have mail held at the post office.
- Never simply discard "pre-approved" credit offers you received in the mail. Always shred them.

## Protect checks.

- Do not have your SSN, driver's license number or home phone number printed on checks.
- If you have a post office box, use it on checks, so thieves won't know where you live.
- Never allow merchants to write your SSN on your checks. In many states, it's illegal.
- Pick up new checks at the bank, instead of having them mailed to you.

## Protect your trash... destroy unwanted documents.

- Invest in a high-quality crosscut shredder.
- Shred everything that has your name and address on it, including: statements and invoices you don't need to keep; all receipts; return address stickers; envelopes, catalogs; neighborhood association lists; and pre-approved credit offers.
- Make sure that any shredding services you use at work take the same amount of care to destroy sensitive documents as you do.
- Take your trash out on the same morning that your removal services are scheduled to come. Don't give thieves time to go through your trash and find any personal information left behind.

## Protect your passwords and PINs.

- Don't use the last four digits of your SSN, your mother's maiden name, your date of birth, your middle name, your child's name, your pet's name, or anything else easily discovered or guessed.
- Discourage your bank from using the last four digits of your SSN as your default PIN. If they do, change it.
- Use a combination of letters and numbers and change your passwords frequently.
- Memorize all passwords. Don't record them on anything you carry with you.
- Password-protect computer files that contain sensitive personal or account data.
- Shield your hand when using an ATM or making long-distance calls with your phone cards. Shoulder surfers may be nearby with binoculars or video cameras.
- Ask your financial institution to add extra security to your account.

## Protect credit cards, credit reports and debit cards.

- Minimize the number of credit and debit cards you use, and carry only one or two at a time.
- Cancel unused accounts. They provide additional targets for identity thieves. However, be aware that canceling credit cards may affect your credit score adversely.
- If you expect a new or reissued credit or debit card in the mail and it doesn't show up on time, contact the issuer immediately.
- Check your credit reports as frequently as possible, at least twice a year. Ask for a 3-in-1, merged credit report with a summary from all three credit bureaus. Under the federal FACT Act, consumers are entitled to one free credit report each year from each of the major agencies. For details, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 877.322.8228.
- Enroll in credit monitoring products to monitor activity.
- Enroll in fraud monitoring (public records monitoring) to alert you of attempts to alter or acquire your identity data.
- Each month carefully review your financial statements, bank statements and phone bills (including mobile phones) for unauthorized use.
- Keep a list and/or photocopies of credit cards, bank accounts and investment accounts in a secure place (not in your wallet or purse!). Include account numbers and phone numbers for customer service and fraud departments, so you can contact them quickly if cards are stolen or accounts are abused.
- Avoid using a PIN-based debit card for purchases when traveling or in any place where you aren't completely familiar with the personnel.
- With unfamiliar merchants use a credit card, which is better protected, or elect to use a non-PIN based transaction. PIN-based transactions are easily "skimmed," making your checking account vulnerable to theft.
- Check your Social Security Earnings Statement each year for signs of fraud. You should receive it yearly approximately three months before your birthday.

## Protect yourself while shopping.

- Never toss credit card receipts into a public trash container. Always shred them at home.
- Carry receipts in your wallet, not in the shopping bag.
- Avoid paying by credit card or debit card, if you think the business will treat your data carelessly.
- When paying your bill, watch what waiters, cashiers and bartenders are doing with your credit or debit card. A growing practice among fraudsters is to "skim" your card number to use it later for fraudulent purchases.
- When filling out applications for loans, credit, mobile phones or other services, find out how the company stores and disposes of your files. Some auto dealerships, department stores, car rental agencies and video stores have been known to treat customer applications sloppily. If you are not convinced that your information is safe, take your business elsewhere.

## Protect yourself on Web sites and with email.

- Never open an email spam or other emails from unknown sources. They may contain viruses or other programs that will make your computer vulnerable to intrusion.
- Never click on a link in an email claiming to come from a financial institution or business, and never provide personal or account data in response. The email may be a fake sent by "phishing" scammers.
- Do not put any credit card numbers or any other personal information on any Web site that you are not familiar with and are not sure is authentic.
- Be aware of techniques for redirecting Web site users to "cloned" replica sites without their knowledge, also known as "pharming." Watch for odd error messages, unexpected page layout or content or other strange site behavior.
- Choose companies that provide secure transactions and have strong privacy and security policies.
- If you bank or transact online, watch your accounts closely for signs of fraud. Encourage those businesses to adopt multi-layer authentication (not just user name/password) to protect your accounts and information.
- To keep hackers from stealing information on your home computer: install a firewall; install virus protection software and keep it updated; keep administrative names and passwords updated; set wireless networks to "no broadcast"; and be sure to power down your computer when not in use.
- Before disposing of your computer, remove all storage drives. Do not rely on the "delete" or trash function to remove files containing sensitive information.
- Store personal files and data back-up securely in your home, especially if you have roommates, employ outside help, or have service work done in your home. Be sure to turn on all security settings built into your computer, and password-protect your computer and files with sensitive personal or account data.

## Remove your name from direct marketing lists.

- Permanently remove your name from the pre-approved mail offer lists by calling 888.5OPT.OUT (888.567.8688) or visit: [www.optoutprescreen.com](http://www.optoutprescreen.com).
- Add your name to the National Do-Not-Call Registry by calling 888.382.1222 or visit the main Do-Not-Call Registry website at: [www.fcc.gov/cgb/donotcall](http://www.fcc.gov/cgb/donotcall).
- Add your name to your state's Do-Not-Call list, if it has one.
- Add your name to "name deletion lists" used nationwide by marketers. To find out how, visit: [www.dmchoice.org](http://www.dmchoice.org).
- Whenever possible, say "no" to the sharing of your personal information by your financial institutions, credit card companies, insurance companies and investment firms. And ask them not to send unsolicited checks.