



Email, the Internet, automated teller machines (ATMs), online banking, cell phones, long-distance carriers, and credit cards make our lives more efficient. However, as our lives become more integrated with technology, keeping our private information confidential becomes more difficult. Electronic transactions can leave you vulnerable to identity theft and other types of fraud. Following a few simple tips can help you keep your private information safe.

## Passwords

Passwords are often required to access information from financial, medical, and other institutions. Hackers have sophisticated tools for cracking passwords. Here are some tips for creating and protecting your passwords.

- **Select at least eight characters**, including a combination of letters, numbers, and symbols that you can remember but that others won't easily guess.
- **Do not use your mother's maiden name**, spouse's name, last four digits of your Social Security number, pet's or children's names, or date of birth.
- **Do not use a word** that can be found in the dictionary in any language.
- **Create a new password** for every website or login that requests one. If that is impractical, create a few hard-to-guess passwords and use those at sites you want to keep most secure. Create easier-to-remember passwords to use at less important sites.
- **Change your passwords regularly**—at least once a month.
- **Memorize your passwords**, if you must write them down, don't carry them in your wallet or leave them in an unprotected place, including a computer file.

- **If you have the option of letting your computer remember a password for you**, don't do it.
- **Do not share your passwords** with family members, friends, or colleagues.
- **If you are logging into an ATM or other computer**, make sure no one is looking over your shoulder as you enter your password.

## Personal Identification Numbers

The personal identification number (PIN) is one method used by banks and phone companies to protect your account from unauthorized access. A PIN is a confidential code issued to the cardholder to permit access to that account. You can protect your PIN number by following these tips:

- **Memorize your PIN number** and do not give it to anyone, including family members or bank employees.
- **Never write** your PIN on ATM or long-distance calling cards; do not carry your PIN number in your purse or wallet.
- **When using an ATM machine or public telephone**, position yourself in front of the ATM keyboard or phone to prevent anyone from observing your PIN as you enter it.
- **Do not leave your receipt behind** when you use an ATM machine; criminals can use them to get your account number.
- **If a bank or other institution assigns you a PIN number** that is the last four digits of your Social Security number, have it changed to a new number.

## Social Security Numbers

Some businesses and government agencies believe that using your Social Security number (SSN) is the most accurate way to store and retrieve information. But your Social Security number is also the prime target of criminals interested in committing identity theft and other crimes. Therefore, it is essential that you protect your SSN.

- **Release your SSN only when it is absolutely necessary.** Employers need your SSN to report your earnings to the IRS, but law enforcement does not need it to issue you a parking permit.
- **Do not carry your Social Security card** in your wallet or purse unless you need it for a specific situation, such as the first day of a new job.
- **Do not print your SSN** on checks or business cards.
- **If possible**, do not put your SSN on job applications.
- **If asked to provide your SSN online**, look for the closed padlock symbol on the bottom of the page, and read the company's privacy policy on how it safeguards your personal information.
- **Do not respond to unsolicited electronic mail messages** in which your SSN and other personal information are requested. No reputable company or government agency sends unsolicited email messages to request sensitive personal data.
- **If a private business requests your SSN**, suggest alternatives like your driver's license number (unless your driver's license number is your SSN).
- **If your state's Department of Motor Vehicles** uses the SSN as the driver's license number, ask for an alternate number.