

Each year more than six million residential burglaries occur throughout the United States. That's one every ten seconds! In addition to the worry of home burglaries, we now also need to concern ourselves with computer hackers and personal identity theft. Listed below are some things that you can do to reduce your chances of becoming a victim.

Home Security Checklist

- Have home security system professionally installed that offers a 24 hour monitoring system. Make sure to post the home system stickers and window decals: this should alert and deter would be intruders.
- Never stop mail or newspaper deliveries, it signals that you are away. Have a neighbor pick up all deliveries if possible.
- When recording your answering machine message, do not state that you are not home or out of town.
- When leaving for an extended period, put lights and stereo /television on a timer to give the appearance that someone is home.

Exterior/Interior Security

- Replace all locks immediately upon moving into your new home and install deadbolts on all outside doors.
- Secure your sliding glass doors with pins to prevent all horizontal and vertical movement. Also install security film over the glass panes for additional protection.
- Remember to lock all doors and windows.
- Provide remote panic buttons for children and/or elderly residents.
- Never keep garage door openers in cars that are parked outside of your home.

Keep Your Valuables Safe

- Keep your important papers, heirloom jewelry and large amounts of cash in a safe deposit box.
- Engrave your valuables with your social security number or drivers license number.
- Store jewelry, firearms, furs and like in a small closet with a non-hinged solid core door that has a deadbolt.
- When purchasing new electronic equipment, breakdown cartons before discarding them. This way you avoid advertising your new purchase to the entire neighborhood and drive-by observers.

Computer Security

Computer security is the process of preventing unauthorized use of your computer.

- Use of anti-virus software on all Internet-connected computers. Be sure to keep your anti-virus software up-to-date.
- Use of some type of firewall product, such as a network appliance or a personal firewall software package.
- Turn off your computer or disconnect its Ethernet interface when you are not using it. An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network.
- Use software backup tools if available, and store the backup disks somewhere away from the computer.

Identity Theft

Identity theft occurs when someone uses your personal information without your permission to commit fraud or other crimes. While you can't entirely control whether you will become a victim, there are steps you can take to minimize your risk.

- Shred financial documents and paperwork with personal information before you discard them.
- Protect your Social Security number. Don't carry your Social Security card in your wallet or write your Social Security number on a check. Give it out only if absolutely necessary or ask to use another identifier.
- Don't give out personal information on the phone, through the mail, or over the Internet unless you know who you are dealing with.
- Never click on links sent in unsolicited emails; instead, type in a web address you know.
- Don't use an obvious password like your birth date, your mother's maiden name, or the last four digits of your Social Security number.