

## SECURITY AWARENESS INFORMATION

### Computer and Electronic Security

There are so many tools available to assist in managing our lives. New technology has brought increased risk of fraud. Listed below are some tips to help protect you from being victim.

- Always set a password on your phone and computer
- Never share your passwords with anyone
- Always store your written login information in a secure place
- Do not store passwords on the front of your computer, under the keyboard, under the mouse pad, in sight when the desk drawer is opened, in a file labeled "Passwords", or on the rolodex on the desk
- Never use a public computer to log into your bank account or credit card accounts. The website and your login information will be stored in the computer for a hacker to retrieve it.
- Never leave the following items in your locked car in plain sight: phone, computer, briefcase, or paper items that have your name and address or personal information (mail)

### Fraud and Scams

ID theft and fraud continue to rise each year at an alarming rate. Listed below are best practices to help protect you from becoming a victim:

- Never give your personal or bank information over the phone to a caller
- Never use an ATM that is not owned by a bank located in convenience stores, malls or airport
- Never respond to any offer that involves depositing checks and keeping a portion of the money. The checks are typically fake and you could lose the money.
- If you feel that you are a victim of fraud or ID theft, report it to the bank. Call customer service at 773-769-2899
- If it sounds too good to be true it probably is. Ask questions and confirm before responding

### Consumer Protection Resources

- [www.fakechecks.org](http://www.fakechecks.org)
- [www.onguardonline.gov](http://www.onguardonline.gov)
- [www.idtheftcenter.org](http://www.idtheftcenter.org)
- [www.annualcreditreport.com](http://www.annualcreditreport.com)