Online Security

Things To Remember:

- Create secure passwords. Keep them private. Change them regularly.
- The strongest passwords look like a random string of characters to attackers. Use a combination of letters, numbers and symbols.
- Update your firewall, virus protection, and browser software regularly.
- Use e-mail software with built-in spam filtering. Keep filters current. Don't open e-mails or attachments if you don't know the sender. Limit sharing e-mail or instant message addresses.
- When doing your online banking and shopping only deal with known, reputable vendors. Before doing business, look for and verify the company's physical address, not a Post Office box. Request a catalog by mail. Speak with a company representative over the phone.
- Don't fall for phishing, mishing, vishing, or other social engineering schemes.
- Back up all your valuable data and keep the backups under lock and key.
- Back up anything you cannot replace easily. The following are some storage devices and locations to consider. External hard drive, CD, DVD, USB flash drive, Online backup and storage service.
- Eradicate personal data from your computer before donating or disposing of it. Remember, manually deleted computer files, may still be recovered by an identity thief. To remove files, search for "file shredder" or "secure file deletion" to find a program that is compatible with your version of Windows and other software. Call the computer manufacturer's technical services department and ask how to delete personal files. A third option is to have reputable computer engineer safely overwrite your files from your hard drive.

Many easy to read safety and security articles can be found at www.microsoft.com/protect