

Internet Security Tips

This is a simple and quick guide for better Internet Security.

Protect Your Identity-----

- Be aware that there are "phishing" or fraud schemes sent via email or web sites posing to be legitimate (banks, credit card companies, online auctions, etc). The "spoofed" sites are designed to trick consumers and collect personal information for identity theft purposes. If you receive suspicious email, don't input personal information, but rather contact the company from which the email was received to report the suspicious email.
- Install firewall software on your computer to prevent unauthorized individuals or information from entering your computer system.
- Frequently run an updated anti-virus program on your computer and apply all security patches for your computer operating system.
- When performing secure online transaction, look for the padlock symbol in the lower right corner of your web page and the https:// denotation in the web page address. This will insure that your online session is in a "secured" environment and the personal information you enter will not be intercepted by snooper.
- Use a password on your computer to prevent unauthorized individuals from accessing your information.
- Change your passwords regularly.
- Avoid using AutoComplete function in your browser for sensitive information.
- Avoid using Internet Banking at Internet Cafes, Libraries, and other public sites to avoid your information from being copied, traced or reentered after you leave.
- Reputable companies will not ask you for your password through e-mail or over the telephone.

Secure Your Passwords-----

- Keep your passwords confidential. If you were to record the information, safeguard and protect the information.
- Avoid using the same password in different websites or applications. Some websites store your password in clear text format, your password will be exposed to the sites' owner. If you want to minimize the sets of password to remember, categorize your passwords to different levels of security. For example, highest security level, such as Internet Banking, critical online transaction, etc, and lower security level. Do not share passwords for highest security level applications.
- Do not choose a password that is easily guessed, like your telephone number, date of birth, or other associated data
- Do not use sequential numbers. Use an alphanumeric combination.