Technology Literacy Class – Cyber Safety for Seniors

- **Install security software and update it regularly.** Install and activate anti-virus, anti-spyware software and install a firewall.

- **Turn on automatic updates so all your software receives the latest fixes.** New viruses and spyware are created every day, so it is important that your software is up-to-date and can detect new threats.

- **Set strong passwords,** particularly for important online accounts and change them regularly - consider making a diary entry to remind yourself.

- **Be suspicious of emails from people you don't know, particularly if they promise you money, good health or a solution to all your problems.** The same applies for websites. Remember, anything that looks too good to be true usually is.

- **Stop and think before you click on links or attachments in emails**. Spam emails often look legitimate but they can be used to carry viruses and other malicious software.

- **Stop and think before you share any personal or financial information-about you, your friends or family.** Don't disclose identity information (drivers licence, Medicare No, birth date, address) through email or online unless you have initiated the contact and you know the other person involved.

- **Before disposing of your computer, remove all traces of your personal data.** Special wiping software can be downloaded or purchased to help you clean your hard drive.

- **Keep yourself informed about the latest cyber security risks.** Subscribe to email notification services that keep you informed about the latest cyber security risks and solutions. See our Alert Service.

- **Make sure your computer is secure**-follow the advice in the Secure your computer section of this website.

- **Set strong passwords, particularly for important online accounts and change them regularly**-consider making a diary entry to remind yourself.

- **Stop and think before you share any personal or financial information-about you, your friends or family**. Don't disclose identity information (drivers licence, Medicare No, birth date, address) through email or online unless you have initiated the contact and you know the other person involved.

- **Don't give your email address out without needing to**. Think about why you are providing it, what the benefit is for you and whether it will mean you are sent emails you don't want.

- **Be very suspicious of emails from people you don't know,** particularly if they promise you money, good health or a solution to all your problems. The same applies for websites. Remember, anything that looks too good to be true usually is.

- **Limit the amount and type of identity information you post on social networking sites.** Don't put sensitive, private or confidential information on your public profile.

- **When shopping online use a secure payment method such as PayPal, BPay, or your credit card.** Avoid money transfers and direct debit, as these can be open to abuse. Never send your bank or credit card details via email.

- **When using a public computer, don't submit or access any sensitive information online.** Public computers may have a keystroke logger installed which can capture your password, credit card number and bank details.
- **Encrypt sensitive information.** If you keep personal or financial information on your computer, consider taking steps to encrypt and protect sensitive files and folders.