5.2 Top-10 Tips To Keep You Safe Online

Topic 5: Tips & Safeguards

The Internet can be a complicated place, not just for seniors, but for everyone! Below are some tips on how to stay safe online. If you find some of the tips confusing that is okay! Don't be afraid to ask someone for help.

- 1. Protect your passwords and change them regularly.
- 2. Install anti-virus, anti-spyware and Internet firewall tools purchased from trusted retailers or suppliers such as Staples.
- 3. Be wary of downloading free files, programs, software or screensavers and avoid unwelcome messages (e-mail, internet pop-ups).
- 4. Never send personal and/or financial information by e-mail.
- 5. Ensure that you are in a secure environment when doing financial transactions online- look for the closed-lock or unbroken-key icons on your browser when entering credit card or other sensitive data.
- 6. Protect your Internet connection, this is especially important if you are directly connected to the Internet for an extended period of time through a cable modem or digital subscriber line (DSL). Disconnect from the Internet when you are finished. If you are not sure what type of connection you have- disconnect anyway.
- 7. If you use wireless internet in your home, make sure you protect your connection with a password. Don't share this password with people you don't know.
- 8. Be sure to log-out or sign-out of secure sites when you are finished, don't simply close your browser.
- 9. Clear your cache when you visit websites, the website addresses are stored in the cache, or memory, of your computer. Make sure you clear the cache of your browser after visiting secure sites so that nobody else can view any confidential information you may have transmitted. The steps for doing this are different for each browser (Firefox, Explorer, Safari), so it is best to do a google search to find the steps to do this.
- 10. Be cautious when using free wireless Internet connections in public places. While many are legitimate free WiFi networks made available by airports, resorts and coffee shops, some may be set up by criminals and using them could allow the fraudsters to access your personal information. Always check with the staff first to make sure you are connecting to the right wireless network. And even if you are connected to the right one, do not use this sort of connection to do any transactions that require you to enter passwords or personal information.

- **11. Check your financial and credit card statements regularly to make sure there is no suspicious activity.**
- **12. Do not use public computers to do financial transactions or to do online banking.**
- **13. If you need help trying to figure out the steps you need to take to protect yourself online, consider finding a legitimate and local company that offers computer servicing and training. It might be worth paying for an hour of their time to ensure you understand how to better protect your online activities.**

Source: (Canadian Bankers Association)