Be Cyber Safe
A Brief Overview for CALL Members

Why are passwords like underwear?
Because you should change them often!

October is Cyber Security Awareness Month in Canada.

This article provides some tips and resources for CALL members. During the pandemic, many have confessed to COVID-cleaning: closets, drawers, photo albums, etc. Maybe this article will be the incentive for you to "clean up your digital presence."

Online scams and identity theft affect many seniors each year and have increased significantly during the pandemic. Little wonder as we spend so much of our daily lives online: email, visiting websites, banking, paying bills, ordering products and keeping in touch with family/friends.

Our CALL Board takes many steps to ensure that the website is protected from technical risks; for example, phishing, targeting phishing and ransomware attacks. (See terminology at end of the article.)

The most important factor for cyber security is YOU. If you heard someone knocking at your door, it is very unlikely that you would open it without knowing who is there. Good practice to keep yourself safe. You can use this same approach to keeping yourself safe online.
Think before you click.

The Government of Canada has a national public awareness campaign created to inform Canadians about cyber security and simples steps they can take to protect themselves online.

You can visit **Get Cyber Safe** to learn more.
https://www.getcybersafe.gc.ca/en

In summary: you can take three steps to increase your safety online.
1. Secure your accounts
2. Secure your devices
3. Secure your connections.

If these actions seem overwhelming, start by taking a few steps at a time. For example, review the information to secure your accounts: passphrases, passwords, and PINs: multi-factor authentication or using a password manager. Set a goal to secure your accounts and become more confident that your information is safe. If, like so many of us, you are tired of choosing passwords that meet all the criteria -- and then forgetting them -- you might consider using a **password manager.** These are apps that help you to create stronger passwords and store them securely in one place so you need to remember only one master password. They remind you not to use the same password on several accounts and to change your passwords regularly.

Just like checking who is at your door, develop some habits to follow when opening a website or an email message.

You can start by checking the security of the URL of a site; this is the Uniform Resource Locator, usually beginning with www and found in the address bar near the top of your browser. Before ordering online, check the security. is it http or is it https -- the latter is more secure. Does it have a padlock? (located near the address bar)

Ask yourself -- where did I get this link? Do I trust the source? For example, if it is in an email, verify that you know the sender.

Remember: think before you click!

Just to prove that seniors can be savvy, enjoy this personal anecdote.

> My aunt moved into assisted living at age 90. One day she left her apartment unlocked to check on her laundry -- just around the corner from her. When she returned she noticed that her purse was missing -- she had the habit of keeping it on a small table near the door. She was about to call the reception when her phone rang. Someone claimed to be from her bank, wanting her to secure all her accounts. For a minute she believed them and wanted to protect her money and identity. When he asked for her PIN number, she became suspicious and she replied: "At my age I don't remember that number but I have it written down somewhere. Please give me your number and I will call you right back." She hung up and called reception and then she called the police. They took the phone number and apprehended two young men-- with her purse and stolen cards in hand. Not all situations will turn out so well. She showed the value of being wary and alert.

Terminology:

Phishing: an attacker masquerades as a trusted entity and dupes a victim into opening an email, instant message or text message. For example, you get an email that looks like it is from Canada Post telling you that your package cannot be delivered until you confirm your address by clicking on a link. What can you do? First, be cautious. Slow down. Read carefully - often the message encourages you to act quickly. Hover over the sender's address to see if it is legitimate. Call the company directly.

Multifactor-authentication: also called two-factor authentication; requires a second step to prove your identity. For example, you login to your bank account and you receive a code on your smartphone that you must enter in order to authenticate yourself.

Ransomware attacks: Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it.