CYBER SAFETY WHEN BROWSING ONLINE

Easy steps older adults can use every day to stay safer on the internet

> **Remember: Pause then Check then Ask**
>
> **If something feels rushed, confusing, or too good to be true, stop before clicking.**

8 Simple Rules for Safer Browsing

1. Visit websites you know

Type the website name yourself or use a saved bookmark instead of clicking random links.

2. Check the web address

Look carefully at the address bar. Scammers often use names that look similar to a real company.

3. Look for the lock icon

For banking, shopping, and sign-in pages, look for the padlock and "https" at the start of the address.

4. Ignore surprise pop-ups

Do not click pop-ups that say your device is infected or that you must call a number immediately.

5. Protect private information

Never give out passwords, banking details, or one-time verification codes through email, text, or phone calls.

6. Use strong passwords

Create longer passwords or short passphrases. Do not reuse the same password for every account.

7. Update your device

Install updates for your phone, tablet, browser, and computer. Updates help fix security problems.

8. Ask when unsure

If a message pressures you, asks for money, or feels confusing, close it and ask a trusted person before acting.

> **Important:** **Real banks, government offices, and technology companies will not ask you to pay with gift cards, cryptocurrency, or secret codes.**

Warning Signs of a Scam

- **You are told to act right away.**
- **You are promised a prize, refund, or urgent problem fix.**
- **The message asks for money, gift cards, cryptocurrency, or remote access to your device.**
- **The sender asks for passwords, banking details, or a code sent to your phone.**
- **The message has spelling mistakes, strange grammar, or an unusual web address.**
- **You feel pressured, afraid, embarrassed, or confused.**

What To Do If Something Feels Wrong

1	Close the webpage or message. Do not click further.
2	Do not send money and do not share personal information.
3	If someone asks to control your device, disconnect the call or session.
4	Call the company, bank, or government office using the official phone number from their real website or from the back of your card.
5	Change your password if you think you entered it on a fake site.
6	Tell a trusted family member, friend, residence staff member, or caregiver.

My Personal Safety Checklist

☐	I will slow down before clicking.
☐	I will not share my password or one-time code.
☐	I will use websites I know and trust.
☐	I will avoid banking or shopping on public Wi-Fi.
☐	I will ask for help if something feels suspicious.
☐	I know who I can call if I am unsure.

Educational reminder: when in doubt, close the page and verify through an official phone number or official website.

GOLDEN RULE *Browse with confidence, pause before you click.*	Questions? Get in Touch! Mila mila@stellarpeaksystems.ca