

MCT Office Services | Online Safety Tips for Seniors



Online Safety Tip for Seniors: Pause Before You Click or Answer

How to Recognize Suspicious Emails, Posts, Texts, and Phone Calls Protecting Yourself from Scams, Fake Links, Suspicious Callers, and Online Fraud

Frauds can happen by email, text message, social media post, or phone call. A scammer may pretend to be from your bank, the CRA, a delivery company, a government office, a friend, or even a family member.

Their goal is often to make you click a link, open an attachment, send money, give personal information, or answer questions before you have time to think.

Why This Matters

Many frauds are designed to make people feel worried, rushed, confused, or afraid. Scammers may use official-looking logos, familiar names, fake phone numbers, recorded messages, or live callers who sound very convincing.

With today's technology and artificial intelligence, fake messages and phone calls can look and sound real. Caller ID can also be misleading. A phone number that appears familiar or official does not always mean the call is safe.

Nothing is ever so urgent that you cannot take a moment to step back, breathe, and verify before acting.

Common Warning Signs

Warning Sign	What to Watch For
Misspelled or unusual website names	The email address or link may look close to a real company but may have missing letters, extra letters, numbers, or unusual characters.
Pressure or fear	The person or message tries to make you panic, feel afraid, or act immediately. Banks, the CRA, and legitimate organizations do not usually pressure you by text, email, social media, or phone call.
Requests for personal or financial information	Be careful if a message or caller asks for passwords, banking details, your Social Insurance Number, credit card numbers, verification codes, gift cards, e-transfers, or other confidential information.
Spelling, grammar, or formatting mistakes	The message may contain errors, awkward wording, unusual spacing, or language that does not sound professional.
Strange or misleading links	The link looks unusual, too long, misspelled, or does not match the company's real website. Do not click if you are unsure.
Suspicious phone calls	A caller asks you to confirm personal information, press a number, call back immediately, buy gift cards, send an e-transfer, or keep the call secret. Hang up and verify using a trusted phone number.

MCT Office Services | Online Safety Tips for Seniors

Warning Sign	What to Watch For
Too good to be true	Be careful with fake prizes, refunds, gifts, investments, miracle offers or promises that sound unrealistic.
Unexpected attachments	Do not open files you were not expecting, especially from unknown senders. Attachments may contain viruses or harmful software.
Unknown or suspicious sender/caller	You do not recognize the person, company, email address, phone number, or social media account. Caller ID, sender names, logos, and email addresses can be fake or manipulated.
Urgent language	Messages or calls that say, "Act now," "Your account will be closed," "Immediate action required," "Urgent," "Time-sensitive," or "Security alert." Scammers use urgency to make you react quickly.
When in doubt, do not click, do not respond, and do not provide information	Go directly to the source. Call the organization using a phone number you know is real, visit the official website yourself, or ask someone you trust before clicking, responding, sending money, or sharing information.

MCT Office Services | Online Safety Tips for Seniors

Important Reminder for Seniors

Nothing is ever so urgent that you cannot take a moment to step back, breathe, and verify before acting.

Scammers often try to make you feel rushed, afraid, or pressured because they do not want you to think clearly. Whether it is an email, text message, social media post, or phone call, take your time before clicking a link, opening an attachment, sending money, answering questions, or sharing personal information.

Once information is shared, money is sent, or a harmful link is opened, there may not always be a “go back” button to undo the damage.

When in doubt, pause, hang up if needed, verify the source, and ask someone you trust for help.

Step-by-Step Safety Check

1	Pause before you act. Do not let anyone rush you. Take a breath and give yourself time to think.
2	Check who sent the message or made the call. Look carefully at the email address, phone number, or account name. Do not rely only on the name, logo, or caller ID.
3	Do not click links right away. Links can lead to fake websites. Type the official website yourself or use a trusted bookmark.
4	Do not share personal information. Do not give passwords, banking information, SIN numbers, credit card numbers, or verification codes by email, text, social media, or phone call.
5	Be careful with attachments. Do not open files you were not expecting.
6	For phone calls, hang up and verify. You are not being rude by ending a suspicious call. Call back using a trusted number, such as the number on your bank card or official website.
7	Ask for help if you are unsure. It is always okay to ask a trusted family member, friend, or support person to help you check before acting.

MCT Office Services | Online Safety Tips for Seniors

Examples

Suspicious email or text:	"Your account has been locked. Click here immediately to verify your banking information."
Suspicious phone call:	"This is your bank. Your account is at risk. Confirm your card number and verification code now."
Why it is suspicious:	The message or caller creates fear, asks you to act quickly, and wants personal or banking information.
Safer action:	Do not click and do not provide information. Hang up if it is a call. Contact your bank directly using the number on your bank card or by typing the bank's official website yourself.

Result: By pausing, checking, and verifying, you can better protect yourself from fraud, identity theft, and economic loss.

NOTE:

You are not being rude by refusing to answer questions, hanging up, deleting a message, or asking for time to verify.

Protecting your personal information is important.

When you are unsure, stop, say no, and check first. That time can make an enormous difference.

Nothing or no one is more important than your wellbeing.