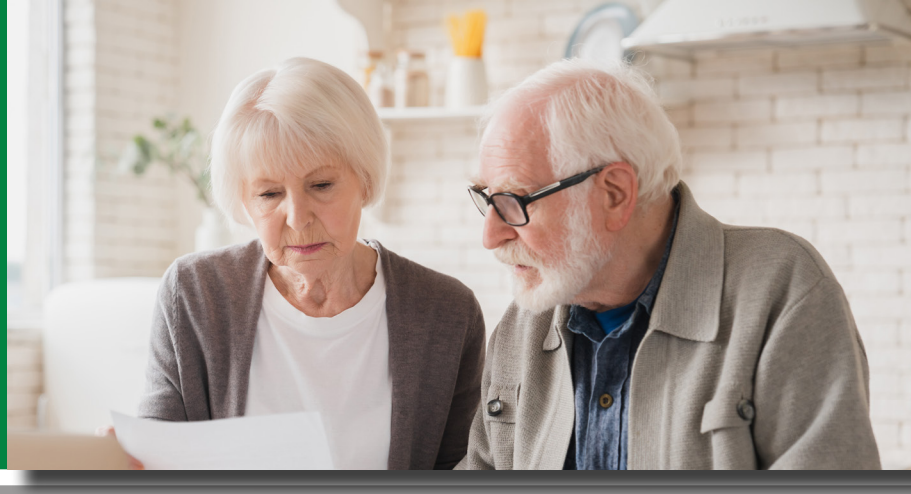
Secure Seniors: A Guide to Technology and Cybersecurity



Ing+McKee INSURANCE

Cyber Criminals

Cyber criminals have become malicious with their threats to seniors, taking advantage of technology that seniors may or may not be familiar with.

At Ing & McKee Insurance, we want to ensure you stay safe and informed in today's digital world. Technology has transformed our lives, but it also brings new risks. Let's explore some essential tips to protect yourself online:

Phishing Awareness:

What is Phishing? Phishing is when cyber criminals trick you into revealing sensitive information (like passwords or credit card details) through emails, texts, or phone calls.

Stay Vigilant: Be cautious when you receive unexpected messages. Verify the sender's identity before clicking any links or sharing personal information.

Examples: Watch out for emails claiming urgent action is needed, misspelled URLs, or requests for sensitive data.

Common examples of phishing scams

Romance Scams:

Seniors looking for love online may encounter fake profiles on dating websites. Cyber criminals create these profiles to exploit personal connections. Here's how to protect against romance scams:

Be Cautious: Be careful about sharing personal information on dating sites.

Unusual Requests: If someone asks for sensitive details (like your Social Insurance Number or mother's maiden name), block them.

Red flags in phishing emails (e.g., urgent requests, misspelled URLs, generic greetings).

No Money Online: Never send money to someone you've only met online, even if they have a convincing story.

Tech Support Scams: Seniors often receive emails or calls from scammers pretending to be tech support representatives. Here's how to handle such situations:

Be Skeptical: If a company contacts you claiming device issues, be cautious.

No Personal Info: Don't provide any personal information. Hang up if they call; delete their email without clicking any links.

Remote Access: Only grant remote access to your computer if you initiated the contact with a reputable tech company.

Grandchild Scam: In this scam, a "family member" (often a grandchild) contacts seniors urgently, claiming they need money or personal information. Here's how to avoid falling for it:

Verify: Always verify the caller's identity. Don't rush to send money or share sensitive data.

Contact Family: Reach out to other family members to confirm the situation before taking action.

Cybersecurity Basics

Strong Passwords: Use unique passwords for each account. Consider using a password manager.

Know Be4 Password Tips Link

Software Updates: Regularly update your devices (phones, tablets, computers) to patch security vulnerabilities.

Beware of Attachments: Don't download attachments from unknown sources.

Stay Safe

Navigating the complexities of today's technology can be daunting. Cybercriminals are ever-present, but with the right knowledge, you can protect yourself and stay worry-free. Remember, you deserve peace of mind in this digital age.

Here is a reputable resource you can check out for tips and education.
Government of Canada Centre for Cyber Security

Want an extra layer of protection?

We've partnered with BOXX Insurance to offer affordable cyber insurance, starting at just $129/year. This coverage is highly recommended for seniors.

Explore Cyberboxx Plans Here

LEARN MORE
403-346-5547
or visit us at **ingandmckee.com**

cyberboxx /HOME + Ing+McKee INSURANCE