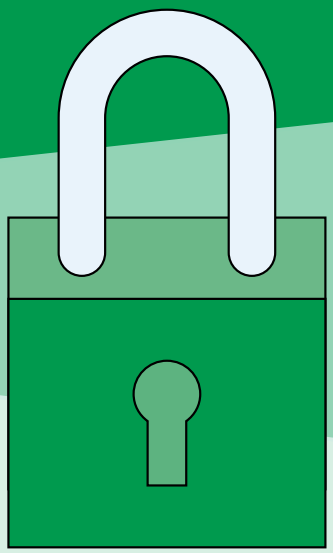
Fraud Prevention Toolkit For Older Adults

Protecting against frauds and scams



CANADIAN BANKERS ASSOCIATION

In partnership with

GETCYBERSAFE.CA

The Canadian Bankers Association (CBA) has created a toolkit to help older adults identify scams and take proactive steps to protect their personal information and finances from fraud.

Banks in Canada are working around the clock to protect their customers from fraud and cyber security threats. They are working closely with each other and with bank regulators, law enforcement and all levels of government to protect the financial system and their customers from financial crime. There are also simple steps to protect yourself and your money from fraud and scams.

Contents

Fraud Prevention Checklist

Protecting your personal information, money and Internet-connected devices from frauds and scams

A regular check in to ensure you're taking the simple, but necessary, steps to keep your money and personal information safe is a great way to proactively protect against frauds and scams.

While banks in Canada use sophisticated technology and layers of security to help protect customers from fraud there are steps that you can, and should, take to protect yourself.

1. Protect your devices

Install anti-virus and anti-malware software to protect your connected devices (like your mobile phone, desktop computer, and tablet) and never skip an update. Install software updates as soon as they are available so you're protected against the latest threats. Even better – automate the updates so they're installed automatically.

2. Create unique, strong passphrases and passwords

Ensure that you create strong and unique passwords for each account and website. This is important since a security breach at one site means your password could be handed to criminals who may try to use it at other sites – this is known as credential stuffing. If you suspect or know that your password has been compromised, be sure to change it on the affected account and any accounts where you may have reused it.

3. Shred papers with sensitive personal information

Destroy all your financial documents before putting them in the garbage or recycling – Safely shred, tear or burn credit card, bank statements and any other documents with sensitive information on them.

4. Limit sharing of sensitive and personal information online

Cyber criminals only need a small amount of your personal information to impersonate you online and commit financial crimes. Be careful what personal data you share online. Don't share your date of birth, home address, PIN or any personal or financial information that could be used to verify your identity in common account security questions. Only share necessary information privately with verified individuals with whom you have initiated contact.

Fraud Prevention Checklist Continued

5. Be careful on the phone

Never give your personal information over the phone, unless you initiated the call. Hang up on calls from phony bank employees or fake members of law enforcement who say they need you to withdraw your money from the bank to help with their investigation. These calls are the first step in launching common scams. Be especially careful to verify calls from phony grandchildren who say they need help following an emergency.

6. Report lost or stolen cards and identity documents immediately

Report lost or stolen credit and debit cards, your driver's license, social insurance number card, passport and other relating personal identification immediately. That way, your bank can block or cancel your card so no one else can use it. Take the time to review your bank account and credit card statements monthly. Check for any charges or withdrawals you don't remember making.

7. Strengthen social media security and privacy settings

Review the privacy and security settings available for all your social media accounts and tighten the default controls. For more details on the security and privacy settings available on specific social media sites you use, visit their corresponding verified websites (applications often have help sources available in settings). Be sure to only accept "friend" requests from individuals you know and review your contacts every few months to ensure all your contacts are relevant.

8. Be wary of downloading free apps, files, programs or software and delete apps you no longer use

Malware (malicious code) like ransomware (that locks you out of your devices or files until a ransom is paid), spyware (that secretly monitors what you do online) and keystroke loggers (that secretly track what you are typing) can be hidden in downloaded files or apps and used to access personal information, such as passwords and financial information. Every few months, check through your devices and delete apps you no longer use so that they don't become a security risk.

9. Don't respond to suspicious emails, phone calls or texts

Your bank will never send you an e-mail asking you to disclose personal information like your credit card number, online banking password or your mother's maiden name. They will also never contact you to ask that you share a one time passcode that you previously requested as part of an account verification process.

10. Be careful on dating apps

Romance scams are on the rise and there are several warning signs that your new relationship could be a scam. Be careful and remember, if your online friend asks you for your sensitive information or money for any reason, end communication. Romance scams depend on a seemingly trusting relationship and a believable story to scam their victims.

Your Fraud Prevention Checklist

- [ ] Protect your devices
- [ ] Create unique, strong passphrases and passwords
- [ ] Shred papers with sensitive personal information
- [ ] Limit sharing of sensitive and personal information online
- [ ] Be careful on the phone
- [ ] Report lost or stolen cards and identity documents immediately
- [ ] Strengthen social media security and privacy settings
- [ ] Be wary of downloading free apps, files, programs or software and delete apps you no longer use
- [ ] Don't respond to suspicious emails, phone calls or texts
- [ ] Be careful on dating apps

Protecting Against Common Scams

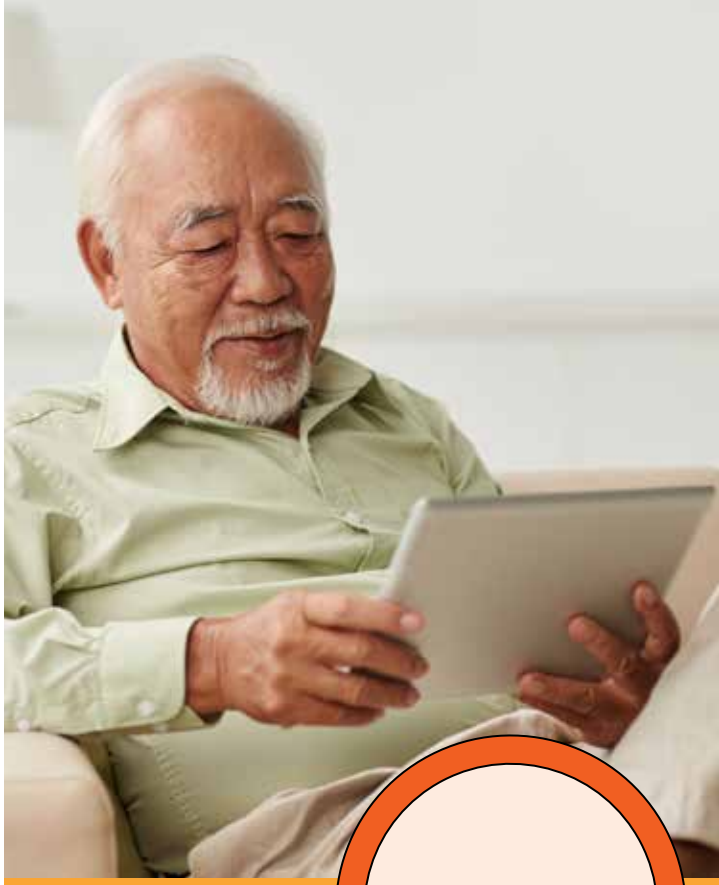
There are several common scams you should be aware of including:

- Email Fraud or Phishing Scams
- Phone or Voicemail Scams
- The Grandparent Scam
- Tech Support Scams
- Romance Scams
- Fake Websites and Applications
- Ransomware
- Emergency Scams

Many scams are variations of a set of tactics fraudsters use to attempt to trick you into revealing sensitive personal information.

Social engineering: Understanding the tactics fraudsters use to trick you

Social engineering is the process criminals use to exploit our basic human urge to respond to urgent requests (like to be useful or help a friend in need) to provide information used to commit financial fraud. Social engineering tactics try to lure us into clicking on malicious links and attachments or into providing sensitive information that can be used to launch cyber crimes or commit financial fraud.



3 ways to spot social engineering techniques

01 Using fear as a motivator. Sending threatening or intimidating emails, phone calls and texts are techniques criminals use to scare you into acting on their demands for personal information or money.

02 Suspicious emails or texts that include urgent requests for personal information are major red flags that someone is trying to trick you into making a quick and regretful decision.

03 Too-good-to-be-true offers or unusual requests. If an online contact offers you free access to an app, game or program in exchange for login credentials or personal information, beware. Similarly, free online offers and links can often contain malware.

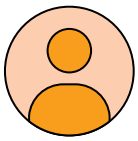
Protecting Against Phishing Scams

Phishing scams are as old as email itself. It's no longer true that spelling and grammatical mistakes in an email are the only common signs of a phishing scam. The increasingly sophisticated nature of these scams means that you need to be on your guard.

Here are a few red flags that the email that just landed in your inbox is a phishing scam:

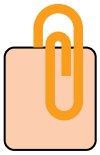
Demands and threats

Is the request for information from a legitimate source? Your bank will never send you a threatening email or call you on the phone demanding information like your password, credit or debit card number, or your mother's maiden name.



Suspicious senders

Check the "from" address by hovering your curser over the sender's name. Some phishing attempts use a sender email address that looks legitimate but isn't. One red flag is when the email domain doesn't match the organization that the sender says they are from.



Suspicious links or attachments

Always be wary of links or attachments that you weren't expecting and more importantly, never click or open them. Scam emails often include embedded links or attachments that may look valid but are hosts for malicious websites or downloadable malware.

Warnings

Warnings that your account will be closed or your access will be limited if you don't reply are telltale signs of a phishing scam.

Protecting Against Phone Scams

Phone scams, also called “vishing,” and text scams, also called “smishing,” can take several forms, but these scams have a few tactics in common.

How the scam works

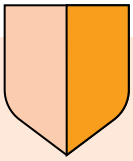
You receive a call or a voicemail from a criminal who might be posing as a government agency or member of law enforcement. The message says you have an overdue balance or outstanding debt or that there is a warrant out for your arrest. Another example of the scam, is a criminal posing as a bank employee asking you to assist them with an investigation with fraudulent activity on your bank or credit card account.

The calls, voicemails and messages seem authentic, but there are often red flags that the communication is a scam:

The calls, texts or voice messages use urgent and threatening language to frighten and bully you into paying the phony debt or providing your login credentials.

The calls or messages include warnings that they’ll contact police if you don’t reply.

The caller demands that you pay your outstanding debt in gift cards, bitcoin or by wire transfer.



How to protect yourself

Banks take extensive measures to protect the personal information you entrust to them and to help you protect it as well. Banks and government agencies will never request payment in the form of gift cards or prepaid cards or debt or a bill.

If you receive a call from a scammer, hang up or delete the voicemail message.

Block the caller’s phone number and report the calls to the Canadian Anti-Fraud Centre to help prevent further scams.

Avoiding the Grandparent Scam

Has your phone ever rung and the person on the other end says they are your grandchild and that something terrible has happened, a car accident for example, and they need money? Receiving a call like this could mean you're a target of what's known as the "Grandparent Scam," a version of the Emergency Scam. These scams are common and it's important that you assess the situation carefully before deciding to help.

How the scam works

You will receive a phone call from someone who starts the conversation with, "Grandma? Do you know who this is?" Thinking it's their grandchild, victims will say "Yes, I know it's you (name of grandchild)."

The caller will then ask for money pretending they were in a car accident or they're under arrest and in jail in another city or country. Sometimes they'll put another person on the phone to act like a police officer, bail bondsman or lawyer.

The victim will then withdraw funds from their bank account and wire money to the "grandchild," or have it ready at home for a courier to pick up.

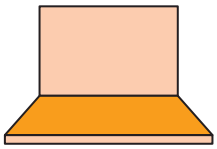
If you've been caught in a scam like this one, call your local police department. Bank staff are aware of these kinds of scams and are trained to pay attention if a customer makes an unusual transaction – for example, withdrawing more money than usual.

How to protect yourself

- Never offer information to the caller. If they prompt you with a question like, "Do you know who this is?" simply say no and have them tell you.
- Press your caller for details. If the person on the other end of the phone is explaining their story, ask them questions about their specific location or have them repeat their story. A criminal will have a hard time recalling details or coming up with them on the spot.
- Ask the caller a few personal questions that your real grandchild could answer but an imposter could not.
- After you hang up, verify the story by calling the parents or other relatives of the "grandchild".
- Never wire money to someone under uncertain conditions. It is nearly impossible to recover or trace money that has been wired.
- Never provide your credit card number over the telephone or Internet unless you are sure about who you're giving it to.

Tech Support Scam

In the very common tech support scam, scammers pose as technical support representatives and try to trick you into paying for unnecessary services or providing access to your computer and personal information.

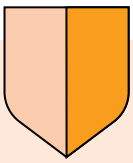


How the scam works

There are a few variations of the tech support scam:

- Sometimes a scammer will call and claim that your home computer has been hacked or is sending out viruses and offer to help you fix the issue for a fee.
- You might see website pop-ups ads that encourage you to call a number to fix a virus detected on your computer.
- Scammers are also sending phishing emails with fake invoices claiming that your subscription to a computer antivirus support service has been renewed. They provide a phone number to call to cancel the service.

Once the scammer has made contact with you, they'll request remote access to your computer where they attempt to steal financial or personal information or they ask you to pay a fee to eliminate dangerous viruses on your computer.



How to protect yourself

- Be suspicious of unsolicited calls. Legitimate tech support companies don't make unsolicited phone calls.
- Do not call a number or click on a link presented in a suspicious form or contact or pop-up.
- Run anti-virus to trace and monitor any vulnerabilities on your device.
- Never log in to your accounts when using remote access or sharing your screen with someone.
- Keep your software up to date. Staying on top of updates ensures your devices are protected from the latest security vulnerabilities.
- Contact a verified company (like the maker of your device) for technical support and further information if necessary.

Understanding the Romance Scam

Romance scams are among the most common scams according to the Canadian Anti-Fraud Centre, costing Canadians more than $50.3 million in losses in 2023.

How the scam works

Typically the victim and criminal will meet through a social media or dating platform. The criminal will then try to develop a relationship with their victim, sometimes spending several months making the victim feel they are in a romantic relationship.

Often the scammer will say that they are in another city or country and that they eventually want to meet the victim in person. The criminal might note that they can't afford to travel and will seek assistance from the victim in covering travel costs.

Another example of this scam includes the criminal noting that there's an emergency, like a sick family member, that they need financial help from the victim to visit the sick individual.

The requests for help are a scam and the money wired by the victim is now in the hands of the criminal.

If you think you may be a victim of a romance scam or any other kind of fraud, it's important to contact the police immediately.

How to protect yourself

Given how common romance scams are, always consider the possibility that your recent match on a dating site might be a scammer. Here are some warning signs that your new relationship may be a scam:

- Your new friend seems comfortable advancing in your relationship fast. Scammers are trying to develop a quick relationship with you so be on your guard when someone professes their love to you.
- Check other platforms for your new friend's profile. Scammers will often not use other platforms or they will have newly activated accounts with very little information to try and mitigate suspicions.
- If your love interest asks you to send money, end communication.
- Does your new friend have an online profile? Look for inconsistencies between what they post, and what they tell you.
- If you receive a message from your friend and they use the wrong name, that may be a red flag. Many of these fraudsters are working on multiple victims at the same time.
- Scammers will claim that they live close to you but that they're working overseas. They do this so that they have numerous reasons to ask for you for money. Be on your guard.
- If you receive a cheque or another form of payment from someone you've met online and they ask you to cash it and send a portion of the funds back to them – don't do it. This is known as the over payment scam.

How to Spot Spoofed (Fake) Websites and Apps

Scammers create online shopping websites and apps that have a similar look and feel to genuine retailers under an intentionally misleading, legitimate-sounding name.

These websites and apps are often just a front to steal your credit card details and sensitive personal information.

Here are a few clues to help you identify a spoofed online shopping site.

Signs of a fake shopping website:

- the site looks poorly designed, unprofessional and has broken links,
- you can't find an address or phone number for the business,
- sales, return and privacy policies are hard to find or unclear,
- the back button is disabled - you get stuck on a page and can't go back,
- you're asked for credit card information anytime other than when you are making a purchase.

Major app store platforms like Apple's App Store and Google's Play Store monitor content and routinely remove malicious apps. But you still need to be vigilant about the apps you download.

Signs of a phony app:

- the name of the app publisher (typically displayed under the app's name) is close to the retail app you're looking for but isn't quite right,
- the app has a poorly written description or doesn't have any user feedback,
- the app requires an excessive number of permissions for installation,
- the app has a lot of pop up ads or you are constantly being asked to enter personal information.

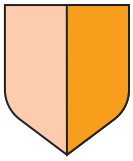
Protect yourself while shopping online

- Shop with reputable and trustworthy retailers that provide a street address and a working phone number.
- When looking for the shopping app of your favorite retailer, visit the retailer's website and look for the link to their legitimate app there – don't just search through the app store.
- Look at the URL of the website to see if it starts with "https" and displays a padlock icon in the address bar. If it begins with "https" instead of "http" it means the site is secured using an SSL Certificate (the s stands for secure).
- Never respond to pop-up messages on a website or app that asks for your financial information.
- Use your credit card and avoid websites and apps that request payment by wire transfer, prepaid debit or gift cards, cash only or through third parties.

Protecting Against Ransomware

Ransomware is a type of malware (malicious software).

Once malware is on your computer, it can lie dormant until the hacker takes control and encrypts your files. When files are encrypted, it is very much like the files are locked, and scammers will demand a ransom payment to decrypt and unlock the files. Do not pay the ransom. These threats are meant to scare and intimidate you. Paying the ransom does not guarantee that they will decrypt your files or that they won't sell or leak the information online.



How you can avoid downloading ransomware

Install reputable, up-to-date anti-virus and anti-malware protection software on all your devices and keep on top of updates.

Take the time to install the latest version of your operating system and applications.

Backup your files frequently to an external source, such as an external drive or cloud-based storage, that is not linked to your computer. If they are linked, your backed-up data could be encrypted too.

Be careful to not click on links or open attachments from unknown senders. Disable macros (code used to automate computing tasks) in documents – you could unknowingly download malware by enabling a macro, clicking on an email attachment, link or online pop-up window.

What to do if you are a victim

It can be very difficult to decrypt your files and remove the ransomware from your computer. If you are the victim of ransomware, you can consider the following:

Don't pay the ransom
It can open you to further and repeat attacks. Criminals can use your willingness to pay the ransom to demand more money.

Disconnect all devices
Ransomware can spread through devices and networks.

Check with your anti-virus provider
If you are familiar with data recovery, you may try to remove the malware yourself. Some anti-virus providers can detect this malware and may have instructions and software to help.

Consult an IT security specialist
A professional may be able to help you remove the ransomware and restore your files if you have them backed up.

Change your passwords
Change your online passwords. That can stop the criminals from further accessing your accounts if they were able to access your passwords.

Report the scam
Alert your local police and the Canadian Anti-Fraud Centre.

Choosing Strong Passwords

CANADIAN BANKERS ASSOCIATION

Choosing strong unique passwords for your sensitive online accounts, like your main email account and your financial accounts, is important since a security breach at one site means your password could be handed to criminals who may try to use it on other sites.

Why are unique passwords so important?

Bad actors use a technique called credential stuffing to gain access to multiple of your accounts. They use automated tools, such as account checker apps, to "stuff" your credentials into as many login pages, such as your bank account, as possible until a match is found. If you're using the same username and password for many different websites, it's more likely that fraudsters will be successful in accessing your accounts.

Your financial institution will have its own specific requirements for secure passwords, but here's an easy way to choose a unique password that's hard to crack and easy to memorize.

Use a passphrase instead of a password

Passphrases are longer yet easier to remember than a password. A passphrase is a memorized phrase consisting of mixed words with or without spaces. For example, basing a passphrase on objects seen in the room around you could look like "LampWindowMatCloset". If the website does not support the characters required for a passphrase, use a complex password based off a memorable phrase.

Phrase:
absence makes the heart grow fonder

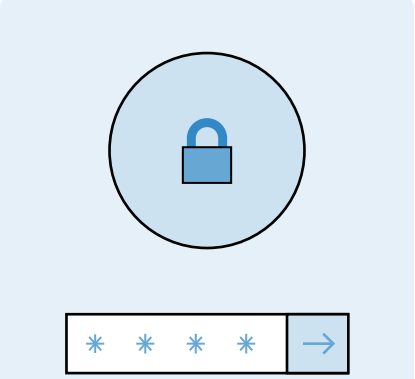
Turn your memorable phrase into a complex password by using uppercase and lowercase letters with numbers and special characters as follows:

Step 1: Determine phrase:

absence makes the heart grow fonder

Step 2: Take the first letters of the words in the phrase:

amthgf



Step 3: Add uppercase letters

AmthgF

Step 4: Expand words, substitute and/or add numbers and special characters and ensure that your password is at least eight characters in length.

Amth3G+F1!

Take additional steps to protect yourself

Strong and unique passwords are the first step in keeping your sensitive personal information protected. Also consider taking advantage of multi-factor authentication for your online accounts when available and keep your computer and device software up-to-date by installing the latest operating systems and security updates.

Protecting Against Financial Abuse

What you need to know and where to get help

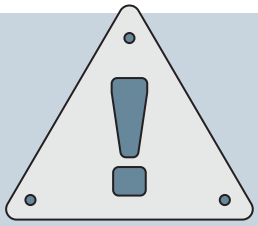
Financial abuse occurs when someone tries to take or control what belongs to you for their own benefit, not yours. This can include your money, your property or your personal information. Financial abuse is unethical and in many cases illegal.

Financial abusers – who are they?

A financial abuser can be a trusted person in your life: a spouse, adult child, grandchild or other family member, caregiver, friend or neighbour.

Examples of financial abuse

A trusted person may be a financial abuser if they:



- put pressure on you to give or lend them money, or to give them access to your financial information,
- use a Power of Attorney for their own benefit,
- force or trick you into signing something, including a contract, Will, letter or guarantee,
- take assets or money from you without permission,
- misuse your bank card or credit card, or have you take out a loan to help them,
- misuse joint bank accounts or pressure you to make your existing account a joint account,
- forge your signature on cheques, including pension cheques, or legal documents,
- sell or transfer your property against your wishes or interests, or
- refuse to return borrowed money or property.

Some warning signs

- A trusted person takes an undue interest or involvement in your financial matters.
- Your statements show account withdrawals or transfers you did not do.
- A trusted person suggests you have your bank statements sent to them
- You start failing to meet your financial obligations, when you've never had problems before.
- A trusted person suggests that you make changes to important contracts – your Will, Power of Attorney, trusts, title to property, deeds or mortgages – that you do not want to make or are not in your best interest.
- You feel afraid of or pressured by a trusted person.

Protecting Against Financial Abuse Continued

How can you prevent it?

- If you are able, do financial transactions yourself. Take advantage of telephone and online banking.
- When planning for your possible inability to manage your finances yourself, allowing a trusted person (or persons) to assist with your financial affairs can be helpful, but you must select your trusted person carefully.
- Powers of Attorney, joint accounts or other arrangements may be useful, but you must be careful. It is generally safer to use a Power of Attorney – which allows a trusted person to act and make decisions for you and obligates them to act in your interest – instead of a joint account – which makes the trusted person the joint owner of your money and investments. Read more about these tools on the CBA's website at https://cba.ca/abuse.
- You can say "no" when someone pressures you for money or to buy something – even family members.
- Make sure you understand every document you sign – do not give anyone your bank card or PIN.
- Set up automated deposits and payments. You can have your income deposited directly into your bank account and have your money sent directly to your necessary bill payments.

Remember, financial abuse is a violation of your rights. It is not your fault, and you can get help. A list of contact information for each province is available on the CBA website at: https://cba.ca/where-to-go-for-help

Please consider obtaining legal advice for all matters related to POAs and planning for incapacity. This text only provides general information and does not constitute a legal opinion. Since the POA rules vary between provinces, the CBA strongly encourages you to seek advice from a legal expert before making any decision in these matters.

Additional Resources

YOUR MONEY SENIORS

The CBA offers a free fraud prevention seminar for older adults as part of its Your MoneySeniors financial literacy seminar program.

Your Money Seniors is available at no cost and consists of three, one-hour seminars designed for Canadians 55 and over. The non-commercial seminars are presented by banker volunteers across Canada who volunteer their time and expertise in their community, and cover three topics:

- **Fraud Prevention** – how to identify and protect yourself from frauds and scams targeted at seniors;
- **Financial Abuse** – what it is and how to avoid it, with an emphasis on avoiding risks associated with Powers of Attorney and Joint Accounts; and
- **Cash Management** – how to prepare yourself financially if you're in or nearing retirement.

Request a fraud prevention seminar today!

CANADIAN BANKERS ASSOCIATION

The Canadian Bankers Association is the voice of more than 60 domestic and foreign banks that help drive Canada's economic growth and prosperity. The CBA advocates for public policies that contribute to a sound, thriving banking system to ensure Canadians can succeed in their financial goals. www.cba.ca

GETCYBERSAFE.CA

Get Cyber Safe is a national public awareness campaign created to inform Canadians about cyber security and the simple steps they can take to protect themselves online. The campaign is led by the Communications Security Establishment, with advice and guidance from its Canadian Centre for Cyber Security, on behalf of the Government of Canada. Getcybersafe.ca

Your bank is also a great resource for cyber security tips and information. Check with your financial institution to learn about the security services, guides and advice they have available to you as a bank customer.

Canadian Bankers Association
Fraud Prevention website:
www.cba.ca/fraud

Canadian Bankers Association
Free fraud prevention newsletter.
Subscribe online.

Government of Canada
Get Cyber Safe campaign
www.getcybersafe.gc.ca

Financial Consumer Agency of Canada
www.canada.ca/en/services/finance/fraud.html