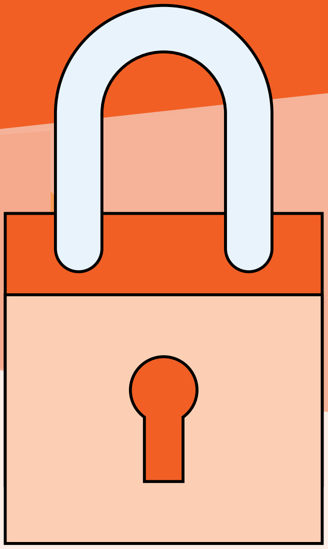
Fraud prevention toolkit for newcomers to Canada

Protecting yourself against online threats



CANADIAN BANKERS ASSOCIATION

In partnership with

GETCYBERSAFE.CA

Updated 2025

A toolkit from the Canadian Bankers Association and Get Cyber Safe to help you understand cyber security threats targeting newcomers and how to develop a cyber hygiene routine to protect yourself.

Banks in Canada are working around the clock on the prevention and detection of 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 you can take to recognize common scams circulating in Canada and protect yourself and your money from financial fraud.

Contents

01 Cyber security 101 for newcomers to Canada

02 Cyber hygiene checklist

03 Protecting against common scams

- 03.1 Email fraud or phishing scams
- 03.2 One-time passcode scams
- 03.3 Phone or voicemail scams
- 03.4 Tax season scams
- 03.5 Fake job opportunities
- 03.6 AI-generated scams
- 03.7 Fake websites and applications
- 03.8 Ransomware

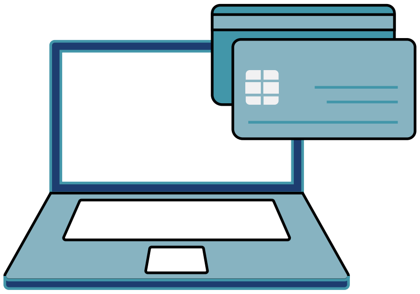
04 Choosing strong passwords

05 How to report scams

06 Additional resources

Cyber security 101 for newcomers to Canada

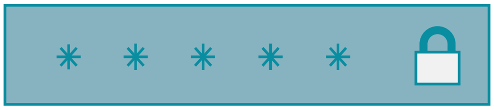
The Internet has made it easier than ever to stay in touch with family and friends back home, conduct business and manage your finances with greater speed, efficiency and convenience.

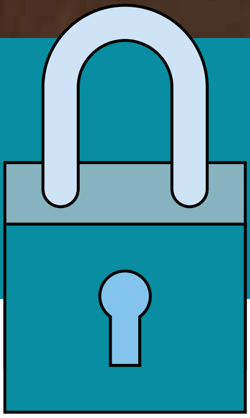


Unfortunately, criminals also use the Internet to try to gain access to personal information such as passwords, personal banking and credit card details and social insurance numbers to commit fraud.

This risk is especially pertinent for newcomers, who may be targeted by scams because they're not as familiar with local laws and common scam practices prevalent in Canada.

Our increasingly connected world means that your personal information is exposed to security risks. Cyber criminals take advantage of the absence of strong cyber security safeguards. The good news is, you don't need to be a computer expert to implement strong cyber hygiene practices.





What is cyber security?

Cyber security is the set of practices that you have in place to protect your devices and personal and financial information. Cyber criminals target individuals to gain information they can exploit to steal money from you.

Cyber hygiene checklist

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

A regular check-in to ensure you're taking the simple, but necessary, steps to proactively protect your money is a great way to 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. Secure your accounts

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. 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. In addition, you should enable multi-factor authentication (MFA) for online accounts when available.

3. Shred papers with sensitive information

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

4. Limit sharing of 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.

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. Claiming they need you to withdraw your money from the bank to help with their investigation is the the first step in launching common scams. Be careful when you receive a call or a voicemail from someone who says they are a government official and that you have done something wrong, such as not filing all the necessary paperwork, and that you need to act immediately or risk losing your immigration or refugee status. It could be a scam.

Cyber hygiene checklist continued

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 to your bank, local police or the Canadian Anti-Fraud Centre as appropriate. 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 free downloads and delete unused apps

Malware (malicious software) like ransomware (that locks you out of your devices or files until a ransom is paid), spyware (that secretly monitors you) 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. Frequently 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 messages

Your bank will never send you an email 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 to watch out for when connecting with someone online. 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 cyber hygiene checklist

- □ Protect your devices
- □ Create unique, strong passphrases and passwords
- □ Shred papers with sensitive information
- □ Limit sharing of 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 free downloads and delete unused apps
- □ 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
- One-time passcode scams
- Phone or voicemail scams
- Tax season scams
- Fake job opportunities
- AI-generated scams
- Fake websites and applications
- Ransomware

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

SOCIAL ENGINEERING: understanding how cyber criminals might try to trick you

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

When it comes to cyber security, even the strongest information security systems are vulnerable when the people accessing those systems are tricked into giving away their login credentials and other personal information.

3 ways to spot social engineering techniques

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

02 Suspicious emails or messages 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

It's no longer true that spelling and grammatical mistakes in an email are a common sign of a phishing scam. The increasingly sophisticated nature of these scams means that you need to be careful.

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 demanding information like your password, credit or debit card number, or your mother's maiden name. Banks and government agencies in Canada will also never demand payment for a debt in gift cards, prepaid credit cards, cryptocurrency or by wire transfer.

Suspicious senders

Check the "from" address. If you hover your curser over the sender's name, you can see the actual email address. 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. Scam emails often include embedded links that may look valid. Hovering your cursor over the links or attachments will often reveal a suspicious URL or filename.

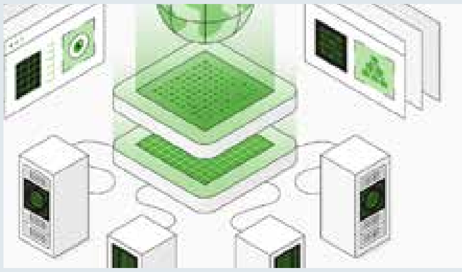
Warnings

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

Unsolicited "thank you" or order confirmation messages

Messages thanking you for a recent purchase you don't remember making or a confirmation for any order you don't remember placing could be scams and are just waiting for you to respond. Always be on your guard.

Test your scam-spotting smarts with the CBA's interactive quizzes: cba.ca/for-canadians/anti-scam-quizzes



One time passcode (OTP) scams

One time passcode (OTP) scams are increasingly used by cyber criminals to attempt to access your accounts.

Here are a few simple tips to avoid getting tricked by OTP scams that you may encounter while attempting to access your accounts securely.

How the scam works

As part of their login process, many websites now require that you provide an OTP, a numeric code, that you can ask to have sent to you. This second step increases security since if your password gets stolen, fraudsters still can't access your account on the site without the time-sensitive passcode.

Fraudsters are now calling or messaging you and pretending to be legitimate organizations such as the post office, bank or other trusted organization, and asking for the OTP that was just delivered to you.

If you think you've been scammed

Banks take extensive steps to protect your personal information entrusted to them and to help you protect it as well. If you think you've been the victim of an OTP scam and provided your financial information to a fraudster, contact your bank immediately.

How to protect yourself

- **Never** share an OTP with anyone who calls you, texts you or emails you asking for the code. The OTP sent to you is personal and unique to you.

- Remember that your bank or any other reputable company will **never** contact you and ask you to share a OTP with them.

Protecting against phone scams

Phone scams can take several forms, but they all have a few tactics in common.

Example on how the scam works

You receive a call or a voicemail from a criminal who is posing as a government official or member of law enforcement. The caller or voice message says you have done something wrong, such as not filing all the necessary paperwork, and that you need to act immediately or risk losing your immigration or refugee status.

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

The calls, texts or voice messages use threatening and aggressive language to frighten and bully you into paying the fake fees or providing your login credentials. A common tactic used by criminals is to claim that you have an outstanding debt with your bank.

The calls or messages include warnings that they'll contact police or revoke your immigration or refugee status if you don't reply.

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

How to protect yourself

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

Remember, Immigration, Refugee and Citizenship Canada will never be aggressive or threaten to arrest or deport you. These calls and emails are always scams.

If you receive a call like this, simply hang up or delete the voicemail message.

You can also block the caller's phone number and report the calls to your local police and the Canadian Anti-Fraud Centre.

More tips here:

Protect your information from scams impersonating government and law enforcement agencies: getcybersafe.gc.ca/en/blogs/protect-your-information-scams-impersonating-government-and-law-enforcement-agencies

Spotting tax season scams

During the income tax filing season in Canada, cyber criminals pose as representatives of the Canada Revenue Agency (CRA) in an attempt to trick you into sending payment for fictious "debts" or into providing sensitive personal information that they can use to commit fraud.

How the scam works

Cyber criminals might send you convincing, and often threatening, messages by text, phone call or email such as:

"Your tax refund is now available. Click here to receive your payment."

"You owe money to the CRA. We will send your file to a collection agency. Contact us now."

"You have a refund of $750 this year. Click here to claim it. Please fill in the online form here."

If you are being targeted or think you may be a victim

If you receive a call or message saying you owe money to the CRA, contact them directly or check your online CRA account. Do not open the link in the message. If you believe you have mistakenly provided your financial information to a cyber criminal, contact your financial institution, the CRA and your local police immediately.

Resources

For information on common Government of Canada-related scams and to learn what to expect if the government contacts you, visit Canada.ca/be-scam-smart.

The CRA will never:

- Send an email with a link asking you to provide personal or financial information
- Send you an email or a text with a link to your refund
- Call you and threaten you with an arrest or that they will send police
- Demand you pay by Interac e-transfer, cryptocurrency, prepaid credit card or gift cards, or use texts or instant messages to start a conversation with taxpayers about their taxes or benefits under any circumstance

Avoiding online employment and job scams

Criminals take advantage of people hoping to find a new job by perpetuating scams with fake employment offers or by involving job seekers in a money laundering operation. Here's how to spot the common red flags of an employment scam.

How the scam works

There are variations of a scam job offer, but there are typically common red flags, including:

- The job offer is unsolicited, arriving as a text or email with promises of easy money
- The "employer" sends you a cheque, often with a fake "contract" and asks you to cash the cheque and send a portion of the money to another person or company – a version of the overpayment scam
- You apply to an online job ad for a position as a "payments processor" or "financial agent" and your job requires you to deposit payments from the company's clients into your bank account and then redirect those funds to a different account according to the "employer's" instructions. These funds could be the proceeds of crime and the cyber criminal has actually hired you to help them hide the source of the funds

How to protect yourself

Always verify that a legitimate company is offering the job. Never offer personal details until you're sure the job offer is legitimate.

Validate the job posting is legitimate by ensuring that the job offer is posted to the company's official website and not only online job boards or by calling the company using a phone number you know is correct and not just provided in the job offer.

Never accept funds on behalf of someone you don't know.

Resources

The Canadian Anti-Fraud Centre provides a listing of common job scams on their website.

Protecting against AI-generated scams

AI-generated phishing scams to voice cloning, the tricks are evolving, but you can still protect yourself. Below are some ways to recognize the signs of a scam and stay safe.

Detecting AI-generated email and text scams

- **Watch for unnatural or overly formal language.** AI-generated scams may use awkward phrases or language that seems just a little too polished. Stay cautious if the message feels off
- **Understand that AI is getting smarter.** As technology advances, scams might become harder to detect, so it is important to stay vigilant
- **Be suspicious of any unsolicited requests for information.** Remember, your bank will never send you an email, or call you on the phone, asking you to disclose personal information such as your password, the one-time passcode to access your account, credit or debit card number, or your mother's maiden name

Detecting AI voice-cloning and video scams

AI can clone voices and images from public videos, using them to impersonate you and request money or sensitive information from your friends and family. Alternatively, your friends and family's voices and images could be cloned to try and trick you into believing they need money.

Watch for abnormal speech patterns. AI-generated speech may sound formal or too precise and there could be long pauses between sentences or in responses.

Remember the common signs and tactics

Even though scammers have new AI tools, their core tricks are the same. Here's how to recognize common scam tactics:

- **Fear as a motivator:** Be wary of threatening emails, calls, or texts that push you to act quickly
- **Urgent requests for personal info:** If you receive urgent messages asking for personal details, pause. Verify the request before responding
- **Too-good-to-be-true offers:** Avoid sharing login credentials, even if the offer seems irresistible. Scammers use AI to create realistic websites and apps to steal your data

Remember, if a message feels intimidating or don't act immediately. Reach out to a trusted friend, family member, or advisor for a second opinion before responding.

How to stay safe online

Protect your devices. Keep your antivirus and firewall software updated to defend against malicious attacks.

Slow down and think. AI allows scammers to craft personalized, convincing messages. Take your time and verify requests before acting.

Seek advice if you're unsure. If you are familiar with data recovery, you may try toremove the malware yourself. Some anti-virus providers can detect this malware and may have instructions and software to help. Report scams. If you ever suspect you have been targeted by a scam, it is important to report it right away. Doing so helps keep you safe, protects others, and makes it harder for scammers to succeed.

How to spot 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 spoofed websites and apps are a front to steal your credit card details and sensitive personal information.

Here are a few clues to help you identify a fake website or app.

Signs of a fake shopping website:

- The site looks poorly designed, unprofessional and has broken links
- The site URL doesn't exactly match the official website, even by a single different character
- The site has an unlocked padlock or uses http (not https). This means it is unencrypted, therefore your information is unsecure. A green, locked padlock and https at the beginning of the URL are signs that the website is using encryption to secure your information
- You can't find an address or phone number for the business, or the phone number on the website doesn't match other reputable sources
- 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 different or close to the official app name 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
- The app shows an excessive amount of data usage or it using data when not opened

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 tiny 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
- Avoid online shopping and banking while using public wifi, or if you must, use a Virtual Private Network

Protecting against ransomware

Ransomware is a type of malware that locks you out of your computer or files and demands a ransom.

When ransomware takes control of your computer or device, it locks you out of that computer or device entirely or certain files. Scammers will demand a ransom payment to decrypt and unlock the computer, device, or 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 turn on automatic updates.

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

Use multi-factor authentication (MFA) on all systems and accounts to have an additional layer of security.

Backup your files frequently to an external source, such as an external drive or cloud-based storage, that is not linked to your computer. Keep highly sensitive information backed up offline using a USB or external hard drive. If they are linked, your backed-up data could be encrypted too.

Be careful to not click on links or open attachments from unknown addresses and disable macros 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
Paying the ransom 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. Use a separate, private network to reduce further spread of potentially dormant ransomware if attempting to recover data or cleanse, reset and update devices.

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 compromised passwords
Change your online passwords for compromised and connected accounts. That will help stop the criminals from accessing your accounts if they were able to access your passwords.

Report the scam
Alert your local police, the Canadian Anti-Fraud Centre and any institutions for accounts that may have been compromised.

Tips on choosing strong passwords for your online accounts

CANADIAN BANKERS ASSOCIATION

Use multi-factor authentication (MFA) on all systems and accounts when available to have an additional layer of security.

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 cyber criminals who may try to use it on other sites.

Why are unique passwords so important?

Using unique passwords for each account and system is important because cyber criminals rake advantage of reused passwords in a technique called credential stuffing. They use automated tools to "stuff" your credentials into as many login pages as possible until a match is found. If you're using the same username and password for many different websites, it's likely that fraudsters will be successful in accessing multiple of your accounts.

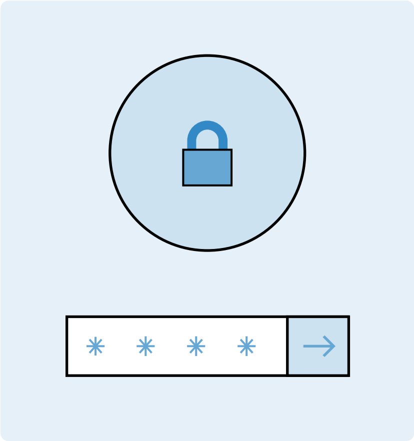
Your financial institution will have its own specific requirements for secure passwords, but here's an easy way to choose a unique password that's hard to crack and easy to memorize.

Use a passphrase instead of a password

Using a passphrase that you associate with that website makes it easier to remember. For example, if you're logging into a photo sharing site, the phrase could relate to images of your friends and family:

Phrase:
absence makes the heart grow fonder

You can turn that phrase into a complex passphrase to meet the security requirement to use letters and 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 passphrase is at least fifteen 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 multifactor 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.

How to report scams

If you ever suspect you have been targeted by a scam, it is important to report it right away. Doing so helps keep you safe, protects others, and makes it harder for scammers to succeed.

Why report scams?

1. It helps to protect others

When you report a scam, you are helping spread the word. Your report could prevent someone else from falling into the same trap.

2. It helps to shut down scammers

Law enforcement and fraud prevention agencies use reports to track down and stop scammers.

3. It can keep your money safe

Reporting a scam quickly can help you secure your accounts and reduce the chance that your money will be stolen.

Common types of scams you can report

Text scams (smishing)

These scams arrive by text to your mobile phone and often look like they are from legitimate companies, like your bank or a federal and provincial government agency.

Phishing emails

These emails try to trick you into sharing personal information by pretending to be from trusted organizations and can contain malicious links designed to help scammers steal your personal or financial information.

Phone scams

Scammers call pretending to be from your bank, a government office, or even a loved one in trouble, asking for money or personal info.

Fake websites

These sites look like real businesses but are actually set up to steal your data, credit card info or money.

How to report scams continued

How to report a scam

1. Report to the CanadianAnti-Fraud Centre (CAFC)

The CAFC collects reports on all types of fraud and scams. By reporting to them, you are helping keep yourself and others safe.

Online Reporting: Use the Fraud Reporting System to report online
Phone: 1-888-495-8501

2. Report to your bank

If you have shared financial information or sent money in a scam, contact your bank or credit card company right away. They can help stop transactions and secure your accounts.

3. Report Spam Texts

You can report spam easily and for free by forwarding it via text message to 7726 (SPAM). Doing so helps to identify new types of spam messages and improve the filters used by telecommunications to block scam texts. Get Cyber Safe has more information about reporting spam text messages to 7726 and instructions for how to report on Android and iOS devices.

4. Report fraudulent websites to the Competition Bureau

If you come across a fake website, report it to the Competition Bureau, which helps enforce laws against misleading marketing practices.

Website: Competition Bureau Fraud Reporting.

5. Report to Local Police

If the scam involves a large financial loss or serious identity theft, you should also report it to your local police department. Most police departments offer non-emergency fraud reporting either online or by phone.

What to do after you report

- **Keep records:** Save all communications related to the scam and document your reports to the authorities.
- **Monitor your accounts:** Keep a close eye on your bank, credit card, and online accounts for any unusual activity.
- **Stay updated:** The Canadian Anti-Fraud Centre regularly posts updates about ongoing scams, so check back to stay informed. You can also subscribe to the Canadian Bankers Association's free Fraud Prevention Tip email newsletter.

Reporting scams is one of the best ways you can protect yourself and others. It only takes a few minutes, but it can make a big difference. Even if you are not sure if something is a scam, it is always better to report it and let the experts investigate. When we all stay alert and report suspicious activity, we make it harder for scammers to succeed.

Additional Resources

Canadian Bankers Association
Scam Prevention website:
cba.ca/scams

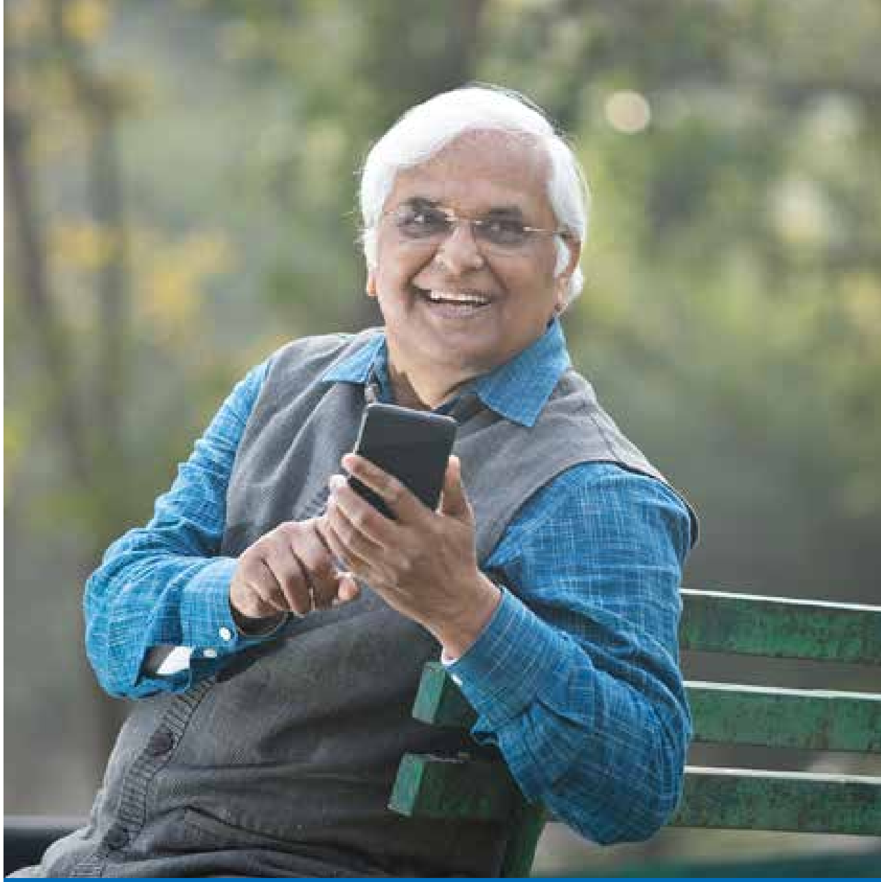
Canadian Bankers Association
Free fraud prevention newsletter.
cba.ca/subscribe

Government of Canada
Get Cyber Safe website
getcybersafe.gc.ca

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

Government of Canada – common immigration and citizenship fraud and scams
canada.ca/en/immigration-refugees-citizenship/services/protect-fraud.html

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. The CBA also has more information and resources for newcomers on their website at cba.ca/article/banking-for-newcomers-to-canada



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. 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