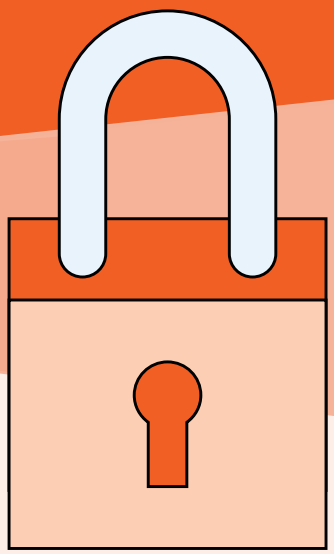
Cyber Security Toolkit for Newcomers to Canada

Protecting yourself against online threats



CANADIAN BANKERS ASSOCIATION

In partnership with

GETCYBERSAFE.CA

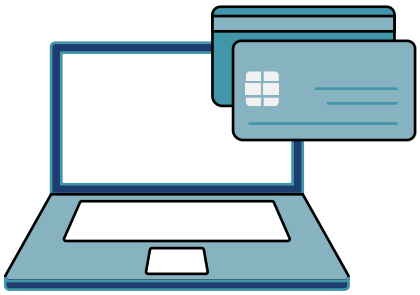
A toolkit from the Canadian Bankers Association and Get Cyber Safe to help you understand cyber security threats targeting newcomers and develop a cyber hygiene routine to protect yourself.

We are all in this together. 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 cyber crime. There are also simple steps you can take to recognize common cyber threats circulating in Canada and protect yourself and your money from financial fraud.

Contents

Cyber Security 101 for Newcomers to Canada

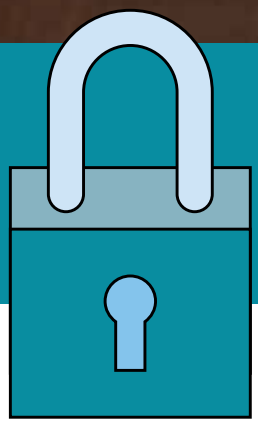
The Internet has made it easier than ever to stay in touch with family and friends back home, conduct business and manage your finances with greater speed, efficiency and convenience.



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 devices and information from cyber attacks

Cyber hygiene is a great way to think about the importance of taking regular steps to proactively protect your connected devices, such as our mobile phones, laptops, desktop computers and smart appliances from cyber threats.

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 on all your connected devices and keep this software up to date. Ensure your operating system has a firewall or download one to help protect your device from malicious intrusions.

2. Install software updates and patches

Install software updates as soon as they're available for all your connected devices. Don't delay downloading as these updates have important security patches and fixes that will protect against known vulnerabilities.

3. Create unique, strong passphrases and passwords

Ensure that you create strong and unique passwords or passphrases for each website and enable Multi-Factor Authentication if it's offered. Unique passwords ensure that in the event of a security breach at one site in which your password is handed to criminals who may try to use it at other sites, they won't be able to access any of your other accounts. If you suspect or know that your password has been compromised, be sure to change it on the affected account and any connected accounts where you have reused it.

4. Schedule regular backups of your data

Back up your files frequently and consider saving critical files to a secure location offline, for example in an external hard drive or on a USB flash drive. This practice helps protect important information from being exposed to cyber threats like ransomware (malware that locks you out of your devices and files for a ransom). Backing up your data ensures you are able to regain access to your important information if your device gets compromised. Always be sure to test your backups to make sure they work.

5. Disable file sharing networks

File sharing networks, often called "peer-to-peer" (P2P), are popular because they allow users to upload and download music, movies, games, documents and other computer programs across global networks. However, accessing these sites is considered a high-risk activity since peer-to-peer sites are commonly used by cyber criminals to distribute objectionable or illegal files and viruses that are disguised to look like innocent downloads.

Cyber Hygiene Checklist
Continued

6. Be wary when downloading apps, files, programs or software

Always be cautious when clicking on a link or downloading a file. Be aware of phishing scams and spoofed websites to protect your devices and information. Malware (malicious software), like ransomware (that locks you out of your devices and files), spyware (that secretly monitors what you do online) and keystroke loggers (that secretly track what you are typing) can be hidden in the downloaded file and used to access personal information, such as passwords and financial information.

7. Limit sharing of sensitive 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 information like your birthdate, address, PIN or any personal or financial information as these are commonly used in security questions to access sensitive accounts.

8. 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. Limit who can access to view your social media accounts and be cautious with what information you share online.

And be sure to only accept requests from individuals you know and review your contacts regularly to ensure all your contacts are relevant.

Your Cyber Hygiene Checklist

- [ ] Protect your devices
- [ ] Install software updates and patches
- [ ] Create unique, strong passphrases and passwords
- [ ] Schedule regular back-ups of your data
- [ ] Disable file sharing networks
- [ ] Be wary when downloading apps, files, programs or software
- [ ] Limit sharing of sensitive personal information online
- [ ] Strengthen social media security and privacy settings

Spotting 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
- Identifying Fake Websites and Applications
- Protecting Against 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 as a motivator. Sending threatening or intimidating emails, phone calls and texts are techniques cyber criminals will use to scare you into acting on their demands for personal information or money.

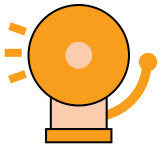
02 Suspicious emails or texts that include urgent requests for personal information are major red flags that someone is trying to trick you.

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

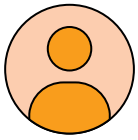
Phishing scams are as old as email itself. It's no longer true that spelling and grammatical mistakes in an email are a common sign of a phishing scam. The increasingly sophisticated nature of these scams means that you need to be on your guard.

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 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 debit in gift cards, prepaid credit cards, cryptocurrency or by wire transfer.



Suspicious senders

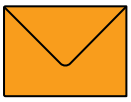
Check the "from" address. If you hover your curser over the sender's name, you can see the actual email address. Some phishing attempts use a sender email address that looks legitimate but isn't – one red flag is when the email domain doesn't match the organization that the sender says they are from.

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

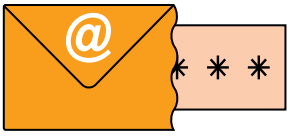
Messages thanking you for a recent purchase you don't remember making or a confirmation for any order you don't remember placing could be scams and are just waiting for you to respond. Always be on your guard.

Test your scam-spotting smarts on the CBA's Cyber Security Awareness Quiz site: cbacybersafety.ca

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.



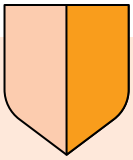
How the scam works

As part of an MFA process, many websites now require that you provide an OTP, a numeric code, that you can ask to have sent to you by text message or by email. 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 your phone by text or email.

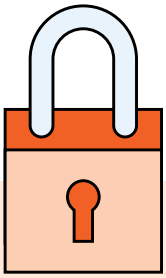
If you think you've been scammed

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** ask you to share an OTP with them over the phone, by text or by email.

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.

Example on how the scam works

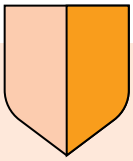
You receive a call or a voicemail from a criminal who is posing as a government official. The caller or voice message says you have done something wrong, such as not filing all the necessary paperwork, and that you need to act immediately or risk losing your immigration or refugee status.

The calls, voicemails, and texts 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 cyber 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 from a cyber criminal, hang up or delete the voicemail message.

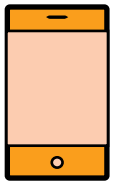
You can also block the caller's phone number and report the calls to your local police and the Canadian Anti-Fraud Centre.

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."

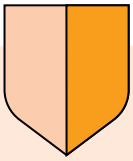
"You have a refund of $750 this year. Click here to claim it. Please fill in the online form here."

If you think you may be a victim

If you receive a call saying you owe money to the CRA, contact them directly or check your online CRA account. 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

Cyber criminals take advantage of people hoping to find a new job by perpetuating scams with phony 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 bogus "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 hired you to launder the funds as a money mule.

How to protect yourself

Always verify that a legitimate company is offering the job.

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.

How to Spot Fake Websites and Apps

Cyber criminals 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 has typos or uses unrelated terms and acronyms,
- 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,
- 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 other forms of payment, such as e-transfer,
- you're asked to offer unrelated sensitve information, such as your Social Insurance Number,
- you're asked for credit card information anytime other than when you are making a purchase.

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).

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

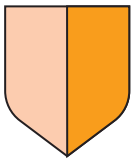
- Shop with reputable and trustworthy retailers that provide a street address and a working phone number.
- Verify the app's legitimacy with the retailer's official website when browsing the app store.
- Look at the URL of the website to see if it starts with "https" and displays a tiny padlock icon 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.

Protecting Against Ransomware

Ransomware is a type of malware that locks you out of your systems and files for a ransom.

Ransomware can lie dormant on your device until the hacker takes control and encrypts (locks) your files. The cyber criminals will demand a ransom payment to decrypt and unlock the files.

Keep in mind that even if you pay the ransom, there are no guarantees that they will unencrypt 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 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:

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 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 password 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 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 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 fraud

Remember, being the victim of a scam or fraud is not your fault. You can help yourself, and others, by taking immediate action.

Contact your financial institution

If you think you may have provided bank account access, credit card information or other financial details to a cyber criminal, contact your bank right away using a phone number that you know is correct (for example the phone number on the back of your debit or credit card).

Contact the police

Report any incidence of fraud to your local police. They may be able to help and you might prevent others from becoming victims of a scam.

Report the incident

You can report frauds and scams to the Canadian Anti-Fraud Centre toll free at 1-888-495-8501 or online.

If you receive a scam e-mail, you should report it and delete it. By reporting fraudulent e-mails you receive to the bank or other company being spoofed, you can help prevent other people from falling victim to the scam. To report a fraudulent email, be sure to send the email as an attachment.

Resources

The government of Canada has additional resources and information on how to report immigration fraud and other types of scams if you're in Canada or if you're outside Canada:

canada.ca/en/immigration-refugees-citizenship/services/protect-fraud/report-fraud.html

Additional Resources

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

Cyber Security Awareness Quiz Site:
cbacybersafety.ca

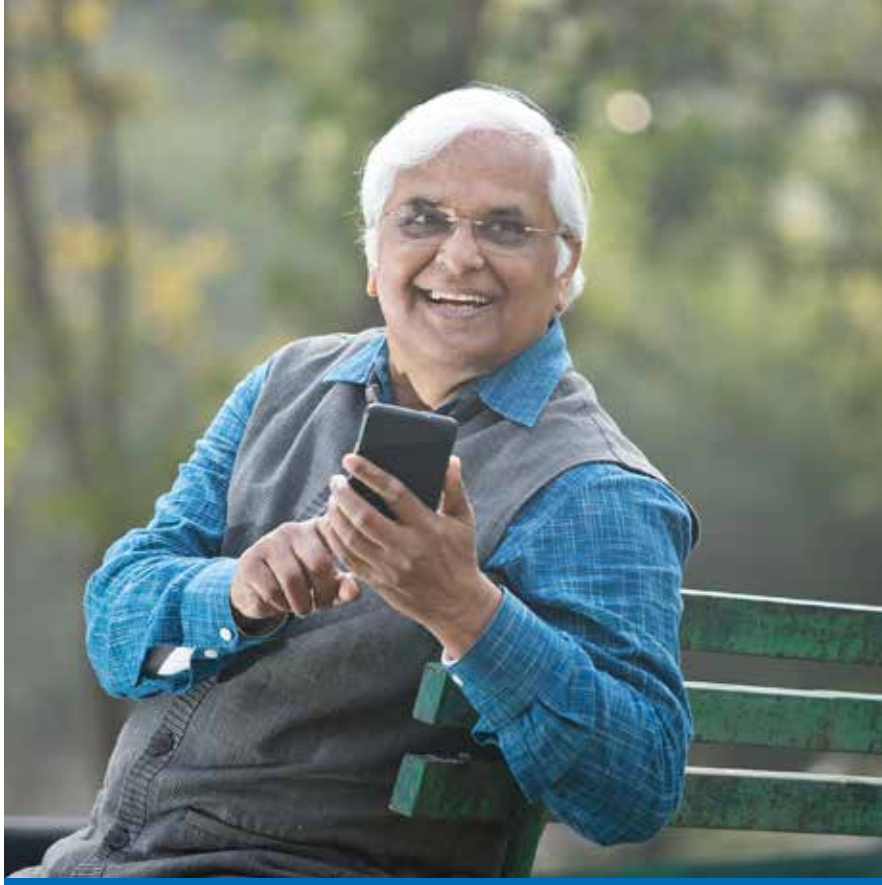
Canadian Bankers Association
Free fraud prevention newsletter.
Subscribe online.

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/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