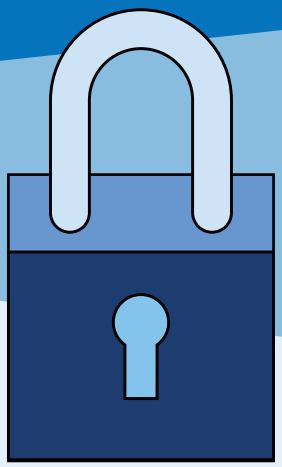
# Fraud prevention toolkit for small and medium-sized enterprises

Protect your small business from cyber threats



CANADIAN BANKERS ASSOCIATION

In partnership with

GETCYBERSAFE.CA

Updated 2026

# A toolkit from the Canadian Bankers Association to help you, as a small business owner or manager, understand cyber security threats and how to protect your business and employees from scams and cyber crime.

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 as a small business owner or manager to recognize common scams and protect yourself and your employees from financial fraud.

## Contents


**01** Cyber security 101

**02** Cyber hygiene checklist

**03** Protecting against common scams

- 03.1 Email fraud or phishing scams
- 03.2 Ransomware
- 03.3 The CEO scam
- 03.4 Business email compromise fraud
- 03.5 One-time passcode scams
- 03.6 Phone scams

**04** Safeguarding customer information

**05** Tips for your employees

**06** How to report scams

**07** Additional resources

# Cyber Security 101

## for your small business

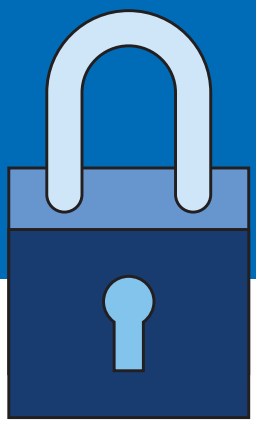
The reality of today's increasingly digital-first economy means that businesses, both large and small, use the Internet to manage their operations, serve their customers and grow their businesses.

Cyber criminals target small businesses because, often, these businesses might not have the resources to implement robust cyber security safeguards. As a small business owner, you need to remain vigilant about cyber security to reduce the risks associated with cyber threats. The good news is you don't need to be a computer expert to implement effective cyber hygiene practices.

### What should you think about when developing a good cyber security plan?

Your cyber security plan should include:

- Procedures on how to protect your business information, computers and networks from cyber attacks
- Mandatory employee training on security principles and how to recognize common scams targeted at small businesses
- Processes and procedures on how to respond to cyber security issues and an ongoing plan to update and adjust your cyber security safeguards to respond to changes with your business' vulnerabilities



## What is cyber security?

Cyber security is the set of protocols, or rules, that you have in place to protect your small business's most important asset – its information. Cyber thieves target small businesses to gain information they can exploit to launch an attack, with the ultimate goal of stealing money from you or your customers.

# Cyber hygiene checklist

## Protecting your business' information, computers, and networks from cyber attacks

Your cyber security plan should include these eight steps to lessen the chance your business will be impacted by cyber threats.

### 1. Install the right security tools

Make sure that you install anti-virus, anti-malware and Internet firewall tools for your business networks and all your connected devices. Keep these programs enabled and update them regularly to protect your business devices from malicious software.

### 2. Create unique, strong passphrases and passwords

Ensure that you create strong and unique passwords and passphrases for all your accounts and website services. Ensure that all employees do the same. Find tips on creating a passphrase on the Canadian Bankers Association website.

Enforce the use of multi-factor authentication (MFA) on devices and accounts. MFA offers an extra layer of security alongside passwords and passphrases, to ensure access is only granted to those who have permission.

### 3. Keep your operating systems up-to-date

Keep your computer operating systems and connected devices updated with the newest version available. These updates have important security patches and fixes that will protect against the latest threats. Even better – automate the updates so they're installed automatically.

### 4. Schedule regular backups of your data

Back up your files frequently to an external secure source. Also ensure that you have clear procedures on how to restore your files from backup and a checklist in place to ensure backups are happening regularly. Be sure to test backups at regular intervals. The Government of Canada's Get Cyber Safe Guide for Small and Medium Businesses – section 7.1 – outlines several options for how to back up data and files for businesses.

# Cyber hygiene checklist continued

## 5. Create guidelines for the type of content that can be shared or uploaded within your organization

Establish clear internal guidelines outlining what employees can and cannot share, upload, or store using company systems, including examples of sensitive information such as customer data, financial records, passwords, and confidential business documents. Ensure staff understand which approved platforms and tools should be used for sharing files and communicating internally, and prohibit the use of personal email accounts or unauthorized applications for business information. Regularly review and update these guidelines as technology and cyber threats evolve, and provide ongoing employee training to reinforce safe information-handling practices.

## 6. Install a Domain Name System (DNS) firewall

Install firewall software to protect your business network from malicious internet traffic. Firewalls scan network traffic and block unwanted traffic from affecting your network. The Government of Canada's Get Cyber Safe website explains how firewalls provide an extra layer of protection for your devices.

## 7. Set up a virtual private network (VPN) gateway for your employees

If you or your employees will be accessing your business' network remotely, set up a VPN to provide a secure and encrypted connection to your sensitive business network. The Canadian Centre for Cyber Security website provides more information about how VPNs work and the types of VPNs that exist.

## 8. Educate your employees about cyber security

Cyber-aware employees are among your strongest lines of defence against a cyber security attack. Focus on having policies and procedures in place for handling your business' information and provide simple, practical and easy-to-implement cyber security tips for your employees to follow. Ensure your employees know what to do if a cyber security incident occurs.

Offer training to employees to help them maintain a strong and current cyber security posture. It helps everyone understand their role in securing themselves and the organization.

## Your cyber hygiene checklist

- [ ] Install the right security tools
- [ ] Create unique, strong passphrases and passwords
- [ ] Keep your operating systems up-to-date
- [ ] Schedule regular backups of your data
- [ ] Disable file sharing networks
- [ ] Install a Domain Name System (DNS) firewall
- [ ] Set up a virtual private network (VPN) gateway for your employees
- [ ] Educate your employees about cyber security

# Protecting against common scams

There are several scams small business owners and managers should be aware of including:

- Email fraud or phishing scams
- Ransomware
- The CEO scam
- Business email compromise fraud
- One-time passcode scams
- Phone scams

And it's helpful to know about the tactics cyber criminals may use to trick you and your employees into revealing sensitive business information.

## SOCIAL ENGINEERING: understanding how cyber criminals might try to trick you and your employees

Social engineering is the process by which criminals exploit our basic human urge to be helpful or to respond to urgent requests, in order to lure us into providing information that can be used 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 or other personal information.

Rather than using technical hacking techniques to conduct a cyber attack, social engineers use manipulation and human psychology to spin a story that they hope we'll fall for.

## 3 ways to spot social engineering techniques

**01** Using fear and urgency as a motivator. Sending threatening or intimidating emails, phone calls and texts are techniques social engineers 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 malicious code.

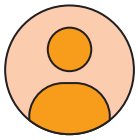
# Email fraud or phishing scams

It's no longer true that spelling and grammatical mistakes in an email are a common sign of a phishing scam. Today's scam messages and emails often look polished and convincing and small businesses can be a target.

**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, requesting information like your password, or credit or debit card numbers. Fraudsters use demanding and threatening language to try and push you into offering them sensitive information.



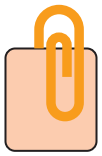
## Suspicious senders

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. Watch for minor letter, symbol or domain changes that aren't easy to recognize.

## Warnings

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

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



## Suspicious links or attachments

Always be wary of links or attachments that you weren't expecting. Scam messages may seem legit and claim to include invoices, delivery notices, or payroll issues. These embedded links look valid but could redirect you to a malicious website or download malicious code onto your device.

## Unsolicited "thank you" or order confirmation messages

Messages thanking you for a recent purchase you don't remember making or a confirmation for an order you don't remember placing could be scams and are just waiting for you to respond. If you're unsure, check your financial statements and do some research on the company claiming you have made a purchase. If a legitimate organization, source their contact information on their official website to reach out. Do not use contact information provided within the suspicious message or click on links to their website, since it could lead to a malicious source.

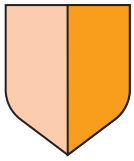
## What business owners and managers can do

- Make phishing awareness part of staff onboarding and training
- Limit employee access to sensitive accounts and systems (allow only required access)
- Create a clear process for reporting suspicious messages, emails and calls

# Ransomware

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

When ransomware takes control of your device, it locks you out of the device entirely or certain files. Scammers will demand a ransom payment to decrypt content and unlock access. 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. It may also leave you and your organization susceptible to future ransomware attacks.



## How you can protect your business from a ransomware attack

Install reputable, up-to-date anti-virus and anti-malware protection software for your devices and networks. Ensure automatic updates are enabled or patch systems frequently.

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

Use MFA on all systems and accounts to have an additional layer of security.

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

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 or clicking on an email attachment, link or online pop-up window.

Educate your employees and offer training to strengthen cyber security at your business.

## What to do if you are a victim

It can be very difficult to decrypt your files and remove the ransomware from your device. If you are the victim of ransomware, 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 from the network.**
Ransomware can spread through devices and networks quickly and unknowingly. Use a separate, private network when attempting to reset, update and recover data and devices to reduce further spread of potentially dormant ransomware.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.

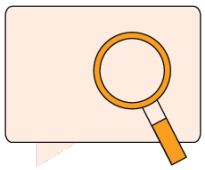
**Consult an IT security specialist**
A professional may be able to help you remove the ransomware and restore your files if you have them backed up.

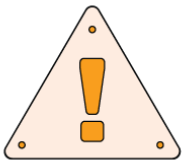
**Change your compromised credentials and online passwords**, particularly for your business bank accounts. That will restrict the criminals from accessing your accounts if they stole your passwords.

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

# The CEO scam

One of the costliest types of business fraud is called the CEO scam, also known as "spear phishing." Unlike mass phishing emails, this scam is targeted. The scammer impersonates a senior executive to pressure an employee into transferring money or sharing sensitive financial information.





## How the scam works

Scammers typically pose as a company executive, such as the CEO or the CFO and contact employees working in the accounting or finance department. The message is designed to appear legitimate and stresses that it is urgent and confidential. The scammer uses social engineering tactics to attempt to gain access to sensitive and financial information.

## Detecting AI voice-cloning and video scams

The use of artificial intelligence (AI) tools can make these scams even more convincing. Scammers can use AI-generated video and audio to impersonate a company executive presenting what looks or sounds like the legitimate individual. Scammers collect audio or video content posted online and use AI-generation tools to create content that appears to be real.

**Signs of AI-generated voice and video scams**

- The video may look slightly unnatural or have stiff facial movements
- The voice may have abnormal speech patterns, sounding formal or too polished with sporadic pauses
- The disguised scammer may try to rush you into sending money or making a decision, just like traditional scams

## How to protect your business

- **Train your team** - Educate your employees about this scam and tell them to be skeptical of urgent or suspicious requests made by email or phone call. Encourage them to communicate directly with their manager if they feel a request seems unusual
- **Always verify requests** - If you or your employees have any suspicions about an email that appears to be from someone at your company, contact them directly by phone to verify the legitimacy of the request
- **Use dual approval for transfers** - Have policies and controls in place requiring more than one officer to approve fund transfers
- **Limit what your share online** - Be careful what you share online (for example, social media and websites). Fraudsters conduct extensive research on individuals and organizations to use targeted information to trick victims into falling for their scams

# Understanding business email compromise fraud

Business email compromise (BEC) fraud includes several types of sophisticated frauds targeted at businesses of all sizes.

## Here's how to spot scams targeted at your business:

### The CEO scam

Spoofed emails that look like they are being sent by senior executives, such as the President, Chief Executive Officer (CEO), Chief Financial Officer (CFO), or other managers are sent to individuals working in the accounting or finance department. The email will attempt to trick the employee into wiring money to a third party and include language making the request sound urgent and confidential.

### Supplier phishing

Spoofed emails that look like they are being sent by suppliers with whom your business has a well-established relationship. These fraudulent emails will request that you provide payment for an invoice by wire transfer to a fraudulent account.

### Information theft

Criminals may also seek sensitive financial information by making legitimate-sounding requests for confidential business information such as tax statements which they can then use to commit fraud.

## Ways to protect against BEC fraud:

### Educate

Educate employees on how to spot these types of scams by making them aware that employee email addresses can be spoofed. Let them know that a major red flag for BEC is a wire transfer request that includes pressure to act or a sense of urgency.

### Verify

The Canadian Anti-Fraud Centre recommends businesses consider a two-step verification process for wire transfer payments so that your business requires two forms of communication to confirm a wire-transfer request is legitimate.

### Be cautious

Take precautions when posting information online or on social media sites about where and when staff, including the CEO or CFO, are on vacation or away from the office.

### Protect

Ensure all software, including anti-virus software, is up to date on all computers and servers in your office(s) and protect your email domain. Use anti-phishing software that aligns with Domain- based Message Authentication, Reporting, and Conformance (DMARC) protocol.

## What to do if your business is victimized

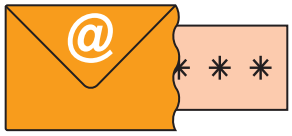
If you learn that a wire transfer is fraudulent, contact your financial institution immediately. You should also report the incident to the police.

# One-time passcode scams: what small businesses need to know

One-time passcode (OTP) scams are increasingly used by scammers to attempt to access your online accounts and small businesses could be a target.

If you manage a business, a OTP scam can put more than just one account at risk. Payroll systems, banking platforms, email accounts and customer data can all be impacted, potentially disrupting operations and costing your business time and money.

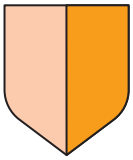
**Here are some practical steps to help protect yourself and your business**



## How the scam works

As part of the login process to access accounts, many organizations now require that users provide a OTP (for example, a numeric code) that is sent through SMS, email or authenticator app to confirm identity. A OTP is a time-sensitive passcode treated as an extra layer of security, after the initial login attempt (for example, username and password). This step in the authentication process is meant to increase security for users if their passwords get stolen, by restricting fraudsters from accessing the account without the OTP.

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



Consider the following if you receive a suspicious call or message requesting a OTP:

- Never share a 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
- Be cautious if you receive a code that you didn't request. This could be a sign a scammer is attempting to access your accounts. Call the organization using contact information on their official website (not from a text or email) to report this security concern
- Remember that your bank, payroll provider, or any other reputable company will never ask you or your staff to share a OTP with them over the phone, by text or by email
- Make sure employees who have access to business systems know how OTP scams work and understand that sharing a code, even once, can compromise the business

## If you think your business has 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.

- Contact your bank and financial institutions immediately
- Change credentials on accounts that have been compromised or are linked to the account
- Ensure you are using unique passwords and passphrases for all accounts to avoid credential stuffing
- Enable multi-factor authentication on accounts

# Phone scams

Phone scams can take several forms, but they all have a few tactics in common. A convincing scam call can lead to unauthorized payments, stolen credentials, or a disruption in the service you provide to your customers.

### How the scam works

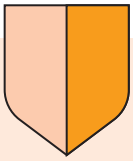
You or an employee may receive a call or a voicemail from a criminal who is posing as a member of law enforcement or a financial institution. The caller says your business has an overdue balance, your company is under investigation or there is suspicious activity on your business' financial accounts

## The calls, voicemails, and messages can sound authentic, but there are often red flags to recognize it is a scam:

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

The calls or messages include warnings that they'll contact police if you don't reply or they may threaten you with legal action.

The caller demands that you pay your outstanding debt in 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 to pay a debt or bill. Consider the following precautions when receiving an unsolicited phone call or message requesting sensitive information.

- Do not provide passwords, account numbers, or verification codes
- Never make payments using gift cards, prepaid cards, cryptocurrency, or wire transfers
- Verify all payment or account-related requests by contacting the organization directly using contact information sourced on their official website
- Make sure employees who handle finances or customer accounts are trained and aware of phone scams and the measures to take to keep sensitive information secure

# Safeguarding customer information

Small businesses can often be targets for cyber thieves because smaller organizations often don't believe they have the resources or knowledge to dedicate to cyber security efforts.

As a small business, one of your most important assets is the personal and financial information you have about your customers and clients. Your customers trust that you will keep their information secure and that you have the proper processes and procedures in place to protect their sensitive information from being accessed by cyber criminals.

To keep information safe, you will need to follow a method for classifying sensitive information and guidelines for your employees on how to handle that information.

## 1. Classify and label your sensitive information properly

The first step in protecting sensitive information that your small business holds is to classify and label it properly. Train employees and enforce the appropriate classification measures to ensure your business' information is handled securely. The Get Cyber Safe Guide for Small and Medium Businesses – section 7.3 – recommends a simple classification model:

### Public information

Available to everyone and anyone, inside or outside of your business. This information requires no protection or special marking or handling, i.e. articles posted to your business' website.

### Restricted information

This information is not public, should be labeled and need to be protected. This could include files and data that are only accessible by employees or service providers, i.e. client records.

### Confidential information

This information is sensitive and needs to be protected with access limited to certain employees. Confidential information must be labelled, protected and restrictions placed on how it can be handled, i.e. company or client financial information.

# Safeguarding customer information continued

## 2. Develop a handling process

Next, develop a process for handling sensitive (restricted and confidential) information about your business and customers. Your protocol should include steps on how to properly store sensitive information properly and outline who in your business can access this information.

## 3. Verify policies and procedures

Ensure you have policies and procedures in place if restricted or sensitive information is ever compromised. Ensure your employees know what to do if a cyber security incident occurs and provide training regularly on cyber security procedures.

## 4. Establish sanitization and destruction systems

Finally, have a system in place for sanitizing devices and destroying sensitive information when it's no longer needed. Proper sanitization and destruction prevents unauthorized access to sensitive information.

**Resources for safeguarding your customers and clients information**

Canadian Centre for Cyber Security

Cyber Security for Small and Medium Organizations

Protecting High-Value Information: Tips for Small and Medium Organizations (ITSAP.40.001)

Baseline Cyber Security Controls for Small and Medium Organizations

Get Cyber Safe

Sections 7.3 and 7.4 of the Get Cyber Safe Guide for Small and Medium Businesses

Office of the Privacy Commission of Canada

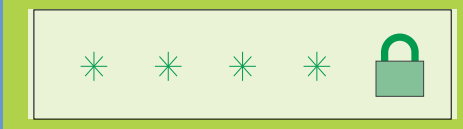
Privacy Guide for Businesses

# Cyber security tips for your employees

CANADIAN BANKERS ASSOCIATION

It's important to build regular and ongoing basic cyber security training for your employees into your cyber security plan. Employees are very often the first line of defence in protecting against cyber security incidents.

To start, focus on simple, practical and easy-to-implement tips for your employees. Protecting against cyber threats is a team sport, so here are some simple ways you can help:



**PASSWORDS: Your first line of defence**

Always use a unique passphrase or password to access your business network.

## Scams 101: red flags that the email you just received is a scam

**Suspicious supplier requests**
Cyber criminals can send emails that look like they're from trusted suppliers. These fraudulent emails will request that you provide payment for an invoice by wire transfer to a fraudulent account. Check the "from" address. If you hover your curser over the name, you can see the actual email address. If the email domain doesn't match the sender's organization, that's a sign of a scam.

**Demands and threats**
Is the information request legitimate? Your bank will never send you a threatening email, or call you on the phone, demanding information such as your password, account verification pins your mother's maiden name or financial card numbers.

**Questionable requests from the business owner or member of senior management**
Cyber criminals can also spoof employee email addresses. A major red flag for Business Email Compromise fraud is a wire transfer request which appears to be sent by the business owner or manager and includes pressure to act or a sense of urgency.

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

**Irregular information requests**
Criminals may also seek sensitive financial information by making legitimate-sounding requests for confidential business information such as tax statements which they can then use to commit fraud.

**Suspicious links or attachments**
Never click on links or open attachments that are suspicious. Always be wary of unsolicited messages including embedded content. Scam emails often include malicious embedded links disguised as a legitimate source. Hovering over the link can help identify the source, but a spoofed link is not always recognizable. If the hyperlinked address doesn't match, the sender's address has irregularities or other information within the email seems suspicious, it's probably a phishing attempt.

### More Tips

- Be wary of phone calls or visits from individuals requesting information about the business or employees. Criminals will often seek out personal information about employees to launch a cyber attack
- When in doubt – double check with a supervisor or a colleague for help
- Report anything suspicious to a supervisor. Very often, you can stop a cyber attack from happening
- If you think business banking information was compromised, report the incident immediately so the incident can be reported to the appropriate financial institution to protect business accounts from being accessed fraudulently

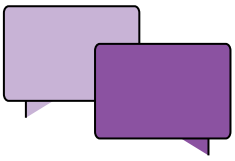
# How to report scams

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 Canadian Anti-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 articles:
cba.ca/scams

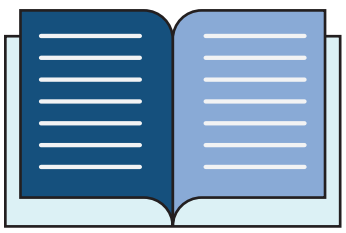
**Canadian Bankers Association**
Free fraud prevention newsletter:
Subscribe online.

**Canadian Anti-Scam Coalition**
standagainstscams.ca

**Government of Canada**
Get Cyber Safe:
Guide for Small and Medium Businesses

**Canadian Centre for Cyber Security**
Baseline Cyber Security Controls for Small and Medium Organizations

**Your bank** may also have additional resources. Check with your financial institution to learn about the security services, guides and advice they have available to you as a small business customer.



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