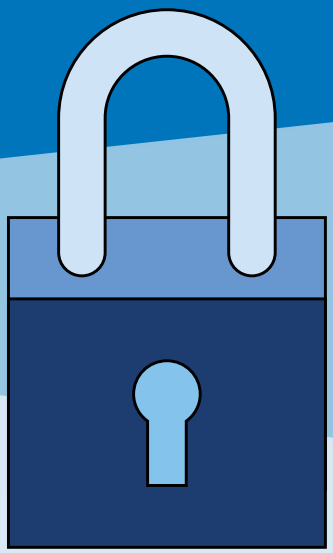
Cyber Security Toolkit

Protect your small business from cyber threats



CANADIAN BANKERS ASSOCIATION

In partnership with

GETCYBERSAFE.CA

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 cyber crime.

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 as a small business owner or manager to recognize cyber threats and protect yourself and your employees from crime.

Contents

01 Cyber Security 101

02 Cyber Hygiene Checklist

03 Spotting Common Scams

- 03.1 Protecting Against Phishing Scams
- 03.2 Protecting Against Ransomware
- 03.3 Understanding Business Email Compromise Fraud

04 Safeguarding Customer Information

05 Tips for Your Employees

06 Additional Resources

Cyber Security 101

for your small business

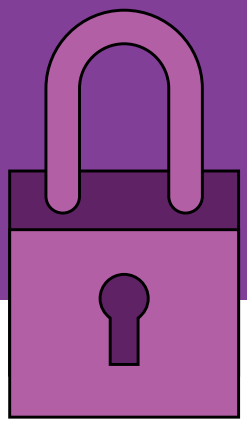
The reality of today's increasingly digital-first economy means that businesses, both large and small, use the Internet to manage their operations, serve their customers and grow their businesses.

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 to 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 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.

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.

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. 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, or allowing employees to access these networks, is considered a high-risk activity since peer-to-peer sites are commonly used by criminals to distribute objectionable or illegal files and viruses that are disguised to look like innocent downloads of popular songs, movies, etc.

6. Install a Domain Name System (DNS) firewall

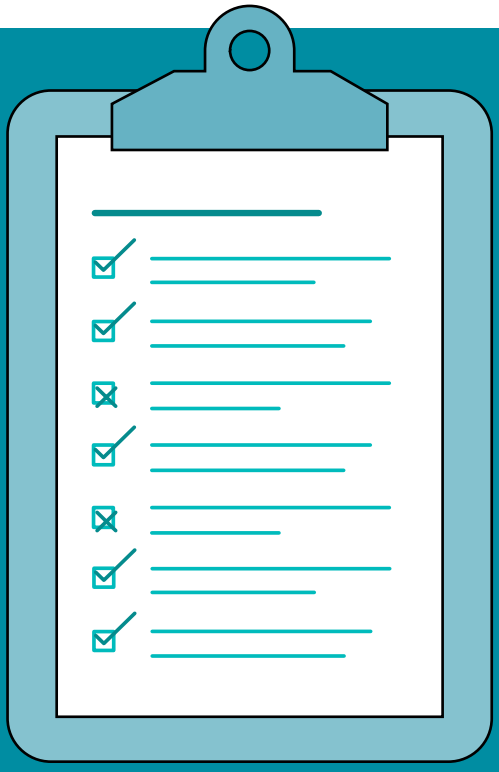
Install firewall software to protect your business network from malicious internet traffic. Firewalls scan network traffic and block unwanted traffic from affecting your network. The Government of Canada’s Get Cyber Safe website explains how firewalls provide an extra layer of protection for your devices.

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.



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

Spotting Common Scams

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

- Phishing
- Ransomware
- Business Email Compromise Fraud

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 believe.

3 ways to spot social engineering techniques

01 Using fear 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.

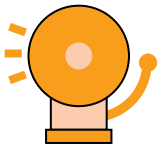
02 Suspicious emails or texts that include urgent requests for personal information are major red flags that someone is trying to trick you.

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

Protecting Against Phishing Scams

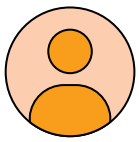
Phishing scams are as old as email itself. These days, however, scammers are using sophisticated techniques to increase the chance that you, or your employees, will be deceived into sending money or financial information to the scammer.

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



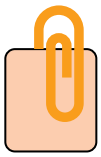
Demands and threats

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



Suspicious senders

Check the "from" address. If you hover your cursor 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, but once you hover over them, the real link will be visible. If the hyperlinked address doesn't match the displayed link or other information within the email, it's probably a phishing attempt.

Warnings

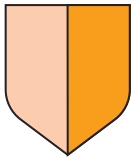
Warnings that your account will be closed or your access limited if you don't reply are a telltale sign of a phishing scam.

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

Protecting Against Ransomware

Ransomware is a type of malware, or malicious software.

Once the malware is on your computer, it can lie dormant until the hacker takes control and encrypts your files. When files are encrypted, it is very much like the files are locked, and scammers will demand a ransom payment to decrypt and unlock the files. 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 protect your business from a ransomware attack

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

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

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

Be careful to not click on links or open attachments from unknown 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.

Educate your employees on the importance of the responsible use of the Internet.

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:

Remove the infected devices from your network. This will prevent the ransomware from spreading.

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, particularly for your business bank accounts. That will stop the criminals from accessing your accounts if they were able to access your passwords.

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

Understanding Business Email Compromise Fraud

Business Email Compromise (BEC) fraud includes several types of sophisticated frauds targeted at businesses both large and small.

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 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.

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. 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.

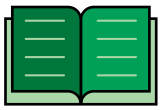
Confidential information

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 should restricted or sensitive information fall into the wrong hands. 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 and has met your organization's information management policies. Proper sanitization and destruction prevents unauthorized access and disclosure of 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

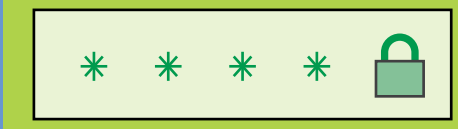
Privacy Guide for Businesses

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 and we're all in this together. 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, credit or debit card number, or your mother's maiden name.

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
Always be wary of links or attachments that you weren't expecting. Scam emails often include embedded links which may look valid, but once you hover over them, the real link will be visible. If the hyperlinked address doesn't match the sender's address or other information within the email, it's probably a phishing attempt. Never click on links or open attachments that are suspicious.

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 obtained, report the incident immediately so the incident can be reported to the appropriate financial institution to protect business accounts from being accessed fraudulently.

Additional Resources

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

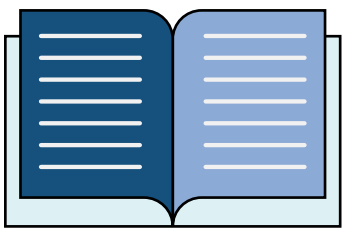
Cyber Security Awareness Quiz Site:
https://cbacybersafety.ca

Canadian Bankers Association
Free fraud prevention newsletter.
Subscribe online.

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. www.cba.ca

GETCYBERSAFE.CA

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