GET CYBER SAFE GUIDE
FOR SMALL BUSINESSES

Communications Security Establishment Canada

Centre de la sécurité des télécommunications Canada

GETCYBERSAFE.CA

Canada

INTRODUCTION

A survey conducted by the British Columbia Chamber of Commerce revealed that nearly two thirds (61%) of Canadian businesses have experienced a cyber security incident[1]. Nearly two thirds!

A cyber security incident can take different forms. You could be a victim of a phishing attack aimed at stealing business information, you may unknowingly download ransomware, or you could get locked out of your business's social media accounts.

When Get Cyber Safe asked what cyber threats small businesses are most concerned about, they responded that they are concerned that a cyber threat will cause work disruptions, financial loss, damage to their organization's reputation or their data being held for ransom[2].

Businesses facing cyber security breaches are not only affected financially, they can also lose the trust of their suppliers and customers.

Assessment

How secure are your small business accounts? Take the 10-question **Get Cyber Safe Checkup** to find out.

STORE

OPEN

If you run a small business, this guide is for you.

[1]Cyber Security and Business Survey, BC Chamber of Commerce https://bcchamber.org/news/new-cyber-security-and-business-survey-reveals-majority-of-businesses-have-experienced-cyber-incidents-but-nearly-three-quarters-didnt-report-it/.

[2]Get Cyber Safe Awareness Tracking Survey, EKOS Research Associates 2021.

Who this guide is for

The Get Cyber Safe guide for small buisnesses is designed for small businesses that:

- don't have a dedicated Information Technology (IT) team
- use social media to promote their business and interact with clients
- use an e-commerce platform to make sales
- are looking for simple steps to keep their business safe online

What you will find in this guide

This guide explains steps you can take to mitigate the risks of cyber threats to help protect your business. These steps will help secure your business assets, sensitive data and investments.

COMMON CYBER THREATS

As a business owner, it is important to be aware of common cyber threats and understand the best way to prevent attacks from impacting your business.

Phishing: Phishing is an attack where a scammer calls, texts or emails you, or uses social media to trick you into clicking a malicious link, downloading malware or sharing sensitive information. Phishing attempts often appear to be legitimate messages from a trusted source (e.g., from a bank or courier company), but are often generic mass messages.

For more information, consult the Canadian Centre for Cyber Security (the Cyber Centre) publication **Don't take the bait: Recognize and avoid phishing attacks (ITSAP.00.101).**

Social engineering: Social engineering is a type of targeted phishing attack where a cyber criminal does research on search engines and social media to learn more about you or your company. Then, they send you a message that looks like it's from a colleague, a supplier, a familiar company or another trusted source. They trick you into sharing sensitive information like passwords, credit card numbers or financial data.

For more information, consult the Cyber Centre's publication **Spotting malicious email messages (ITSAP.00.100)**.

Malware: Cyber criminals can use malware, or malicious software, to infiltrate or damage networks, systems and devices. Once malware is installed on your organization's systems and devices, cyber criminals can gain access to sensitive information.

For more information, consult the Cyber Centre's publication **Protect your organization from malware (ITSAP.00.057).**

Ransomware: Ransomware is a type of malicious software that infects your device and holds your files and data for ransom. The infected device displays a message explaining that your files are inaccessible and you must pay to retrieve your information. But unlike kidnappers in a movie, in lieu of a suitcase full of money, the cyber criminals will demand payment in the form of digital currency that is difficult to trace, such as bitcoin.

For more information, consult the Cyber Centre's publication **Ransomware: How to prevent and recover (ITSAP.00.099).**

Hacking: Hacking is a term used to describe actions taken by someone to gain unauthorized access to a device. With this access, cyber criminals can take control of accounts, such as your business's social media accounts, to access personal and business information, redirect your followers to scams or discredit your business.

For more information, consult the Cyber Centre's publications **Have you been hacked? (ITSAP.00.015)** and **Loss of control of social media channels.**

Back to table of contents

PRIORITIZING CYBER SECURITY

DEFINING ROLES AND RESPONSIBILITIES

Your business should have at least one person handling cyber security. This person would be responsible for the following:

> Learning about threats, trends and security options

> Planning, implementing and maintaining the ten mitigation steps outlined in this guide

> Helping other staff understand cyber security best practices and policies

Using this guide, your business's cyber security lead will have the knowledge and tools to help protect your business from common cyber threats.

OUTSOURCING CYBER SECURITY

Some small businesses may want to use service providers to remotely manage their organizations' IT infrastructure, cyber security and other related business operations.

For more information on working with managed service providers (MSPs) and deciding the best option for your business, consult the Cyber Centre's publication **Choosing the best cyber security solution for your organization (ITSM.10.023)**.

BUDGETING FOR CYBER SECURITY

Taking care of your business's cyber security may involve a financial investment depending on the tools you put in place. Factor in the costs of cyber security when you draw up your annual business plans and budgets. For example, the following applications and services like anti-virus software, password manager and virtual private networks (VPNs) could involve upfront fees or annual subscriptions.

To avoid surprise expenses, it is best to be prepared for costs associated with the following:

> Security tools

> Upgrades or updates

> Technical support

> Training costs

> Contingencies

Contingency funds are important to deal with unforeseen emergencies (such as malware infection).

In some cases, your insurance may cover losses due to a cyber security incident. It is important to discuss your coverage with your insurance provider in advance.
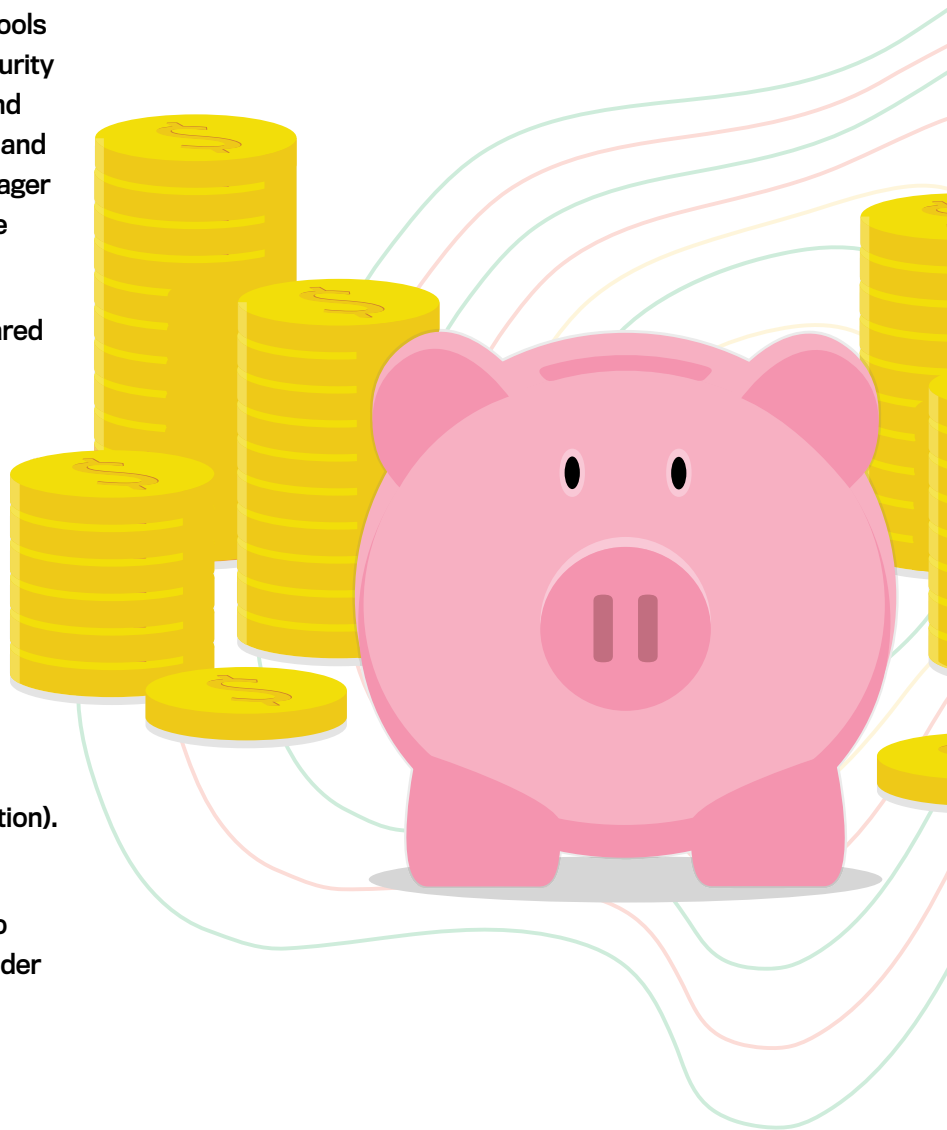
For more information about cyber insurance, consult the Insurance Bureau of Canada's blog on the Get Cyber Safe website: **Does your small business need cyber insurance?**

CYBER INSURANCE

Cyber insurance is a specialized product intended to help businesses manage losses caused by computer networking attacks, such as data breaches and cyber extortion. Cyber insurance can cover a range of cyber events, including:

> breaches of confidential data: the loss of and unauthorized access to confidential or personal information

> cyber extortion: a demand for payment under the threat of restricting your access or compromising your data, such as a ransomware attack

> technology disruptions: a technology failure or denial-of-service (DoS) attack, which prevents access to your online services

Cyber insurance can help cover many costs that arise from a cyber attack, including legal representation, notifying affected parties, hiring a firm to investigate the cause of the breach and restoring damaged or corrupted data.

TEN STEPS TO MITIGATE RISKS

Here are ten steps to take to enhance your business's cyber security. These steps are not in order of importance but include cyber security guidance for the different areas of your business. Consider the following steps when setting up and enhancing your business's cyber security posture.

1 Take stock of assets

2 Secure your accounts and devices

3 Secure your network

4 Develop a backup system

5 Protect customer and sensitive data

6 Enable automatic updates

7 Develop a cyber security plan

8 Train employees

9 Establish an incident response plan

10 Stay up to date

Back to table of contents

1

TAKE STOCK OF ASSETS

Taking stock of your assets is an important first step in securing your business against cyber threats. Create a list for all your business's assets to help keep track and monitor their usage in case of a cyber security incident. Here are some examples of common assets businesses should take stock of.

> **Physical devices** your business uses to connect to the internet such as desktop computers, laptops, servers, routers and mobile devices, such as phones and tablets

> **Physical peripherals**, such as printers, scanners, monitors, keyboards, mouses and docking stations

> **Connected or smart devices**, such as point-of-sale (POS) devices, thermostats, personal assistants, speakers, lights and security systems

> **Physical storage devices**, such as external hard drives, network area storage (NAS) devices and USB keys

> **Digital assets and services** (social media accounts, websites, cloud and online bookkeeping services)

Your asset inventory list should include each of the devices' serial numbers, locations, software license expiry dates and the names and contact information of the people who have access to them.

Template
You can find an asset inventory list template **at the end of this guide.**

Back to table of contents

2

SECURE YOUR ACCOUNTS AND DEVICES

Once you have an inventory of your assets, consider the following cyber security measures to secure the devices and accounts used in support of your business.

Devices

If you use several devices such as desktop computers, laptops, mobile phones and tablets to run your business, consider the following:

> Which devices have access to customer data (e.g., names, addresses, payment information)

> Which devices have access to your business's financial data (e.g., bank account, tax information)

> Which devices have access to proprietary data relating to your competitive advantage (e.g., pricing, margins and patents)

> If employees use their own personal devices to access your business information

Remember that your company cannot manage employees' personal devices to the same extent as business-owned devices. Your company's data is susceptible to vulnerabilities on employee devices that can include malicious software, out-of-date software and lack of security tools.

By providing employees with business-owned devices, your company can manage the usage and make sure cyber security measures are in place.

If it's not possible to supply dedicated business devices for all employees, be sure to set the expectations for what business activities can be done on personal devices.

If your business allows employees to use their own personal devices to handle business information, remember to remove company account access when employees leave your organization. This can be done by developing a Bring-Your-Own-Device (BYOD) policy that outlines the work-related activities that employees are allowed to do on their personal devices.

For more details on BYOD, refer to the Cyber Centre's publication **End user device security for Bring-Your-Own-Device (BYOD) deployment models (ITSM.70.003).**

Back to table of contents

Access, accounts and roles

Make sure that access to programs, software and sensitive data is limited to only those who have a clear business need and only as much access as they need. Sometimes this is done in the software itself and sometimes through the operating system. This is especially important when it comes to administrative access. Limiting access reduces your risk.

Minimize the number of employees with administrative privileges to software, especially important applications and security safeguards. Many cyber criminals target user accounts with administrative privileges because it gives them a high level of control over software and systems.

For more details, refer to the Cyber Centre's publication **Managing and controlling administrative privileges (ITSAP.10.094).**

Social media accounts and other online services often allow you to assign roles to employees within your company account. For example, Facebook has roles for admin, editor, moderator, jobs manager, advertiser and analyst. The roles come with specific access and permissions. Your business can use the roles to control access to client data and financial information.

Passwords and passphrases

Most devices come with a default username and password set by the manufacturer. This is a huge security risk, but one that can easily be addressed by **changing the password** as soon as you get the device. Whenever possible, use a passphrase, which is a combination of four or more random words and a minimum of 15 characters in length. A passphrase should be memorable to you but difficult for a cyber criminal to guess.

If your device or account does not allow for a long passphrase, choose a password made up of at least 12 characters with a combination of upper and lower-case letters, at least one number and at least one special character that is not a letter or number.

It is important to use unique passwords for every device and every account your business owns. This way if one device or account is compromised it won't easily affect others.

Back to table of contents

Password managers

While using a unique password for each device and account keeps a compromised account from spreading, it also makes for a lot of passwords to remember! Use a password manager to help create, organize and remember your credentials.

For more details, consult Get Cyber Safe's **How to choose the right password manager for you.**

Multi-factor authentication (MFA)

Enable MFA on all accounts where it is available. This is a combination of two or more authentication factors. The authentication factors can be a combination of something users know (e.g. password or PIN), something users have (e.g. a smart card or a security key), or something the user is (biometric features like a fingerprint or face scan). Using an additional authentication factor to verify users' identities ensures that even if a cyber criminal gets hold of a password, they will not be able to access the account without knowing the additional authentication factors. For details on MFA deployment, refer to the Cyber Centre's publication **Steps for effectively deploying multi-factor authentication (MFA) (ITSAP.00.105)**.

Smart devices and the Internet of Things (IoT)

IoT refers to the network of everyday web-enabled devices that can connect and exchange information. These smart devices include items like personal fitness trackers, TVs, thermostats or connected cars.

When selecting smart devices for your small business, take the product's security features and privacy policy into account.

> **Security Features:** Some smart device manufacturers design their products to be easy to use and low cost to the consumer. But this can mean that the device's security features are weak or non-existent. When buying a new smart device, think about what data will be transmitted through the device, then research how the device will be protecting that data. At a minimum, check to see if the device will give you the option to create your own strong and unique passphrase or password.

> **Privacy Policy:** Smart devices can capture and transmit a lot of private information about your business, including payment information. So, before you buy a smart device, check to see how the vendor will be protecting the privacy of your information. Reputable smart device vendors will have a published policy that will explain the types of data their device will collect about you, how they will protect the privacy of your data and which companies and advertisers they will share your data with. In short, be sure to look for and understand the vendor's privacy policy and terms of use.

For more information, consult the Cyber Centre's **Internet of Things (IoT) Security (ITSAP.00.012)** and **How is your smart device listening to you? (ITSAP.70.013).**

Back to table of contents

Software and apps

The security in the software and applications your organization uses is very important in maintaining a good cyber security posture. Software can have issues (usually known as "bugs") that can make it unsecure. These bugs can be exploited by cyber criminals and allow them to access your information. Sometimes, software will also carry malicious software – commonly referred to as malware. To maintain software security:

> use legitimate software from reputable vendors that has been tested

> do not use unauthorized versions of software illegally downloaded

> apply security updates (patches) to your software as soon as they are available (**see step 6 to enable automatic updates**)

Website hosting

If your business's website is not properly secured, it could be easily compromised. This could lead to vandalism, disruption of service or the theft of business or client data. Websites vary from business to business, but there are some basic tips to follow:

> If your business uses a web hosting service, make sure they have a security plan and that they:

- scan their web servers and your website for potential issues and then fix those issues to further protect the server and your site

- monitor your website (and any systems) for intrusion or attempted vandalism

- protect your website from intrusion and disruption

- will restore your site to service in the event of a failure or disruption by cyber criminals

> Use generic business accounts like sales@yourbusiness.com to keep cyber criminals from gaining any personal information (from the email name or reaching out with a phishing attack)

> If hosting your website(s) internally on servers belonging to your business, refer to the Cyber Centre's publication **Security considerations for your website (ITSM.60.005)**

Point-Of-Sale (POS) security

It's likely that your business relies on electronic point-of-sale (POS) systems for processing financial transactions. Customers have come to expect the convenience of POS for instant debit or credit card transactions, making it essential to your business.

Your POS systems can be another way for cyber criminals to access your computer networks and it is extremely important to protect them. Cyber criminals can hack into POS systems (using stolen credentials or unpatched vulnerabilities) to steal payment card numbers and the associated personal identification number (PIN), which they can then use to access your customers' accounts.

These are the steps you can take to improve POS security to help safeguard your customers and your business:

> Ensure that your POS system is behind a firewall

> Set up strong encryption for the transmission of all data (e.g., cardholder data) between your POS system and the POS service provider

- check that your service provider has implemented this by default

- ask your POS service provider or a cyber security consultant (with POS experience) for help if you are not sure what to do

> Replace the default username and password to a new username and password that is unique

> Always limit access to customer data only to those employees who have a need to access it and are authorized to do so

> Keep your anti-virus and anti-malware software up to date

3
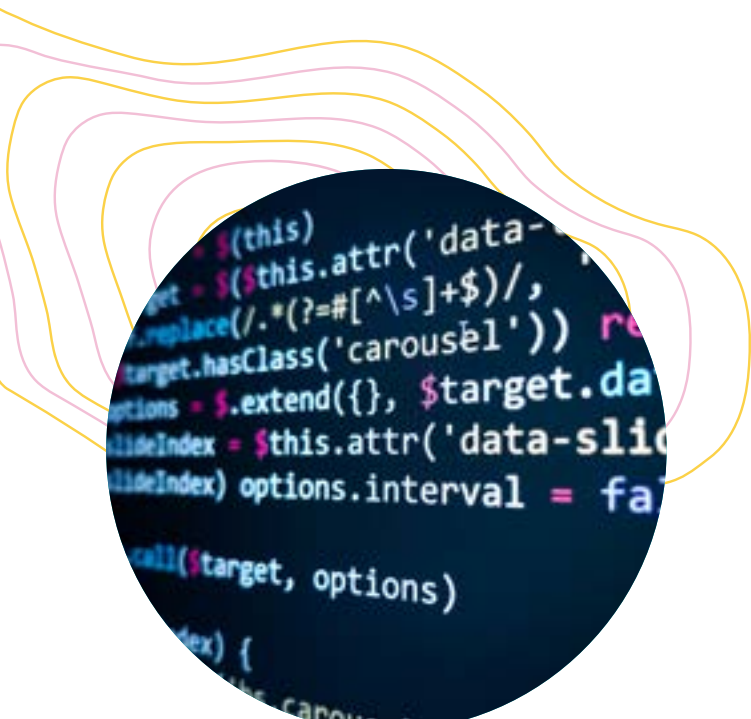
SECURE YOUR NETWORK

Cyber criminals can wreak havoc on business by attacking your network to steal data and perform other malicious activity. Make sure your network is protected at a minimum by a firewall and anti-virus software. You should consider segmenting your network to better protect your systems and data. If you or your employees telework or travel, provide a virtual private network (VPN) connection to connect to corporate resources.

For more details on securing your network, refer to the Cyber Centre's publications **Virtual private networks (ITSAP.80.101)** and the **Top 10 IT security actions: No. 5 segment and separate information (ITSM.10.092).**

Private Wi-Fi network

Securing your business's Wi-Fi network is easier than it sounds. Start by changing the Wi-Fi name and password your router came with. Make sure the network name doesn't include any personal information and use a strong, unique password or passphrase. Then, create a separate Wi-Fi network for guests and smart devices. This adds an extra layer of protection for your more sensitive network since smart devices are often more vulnerable to cyber threats.
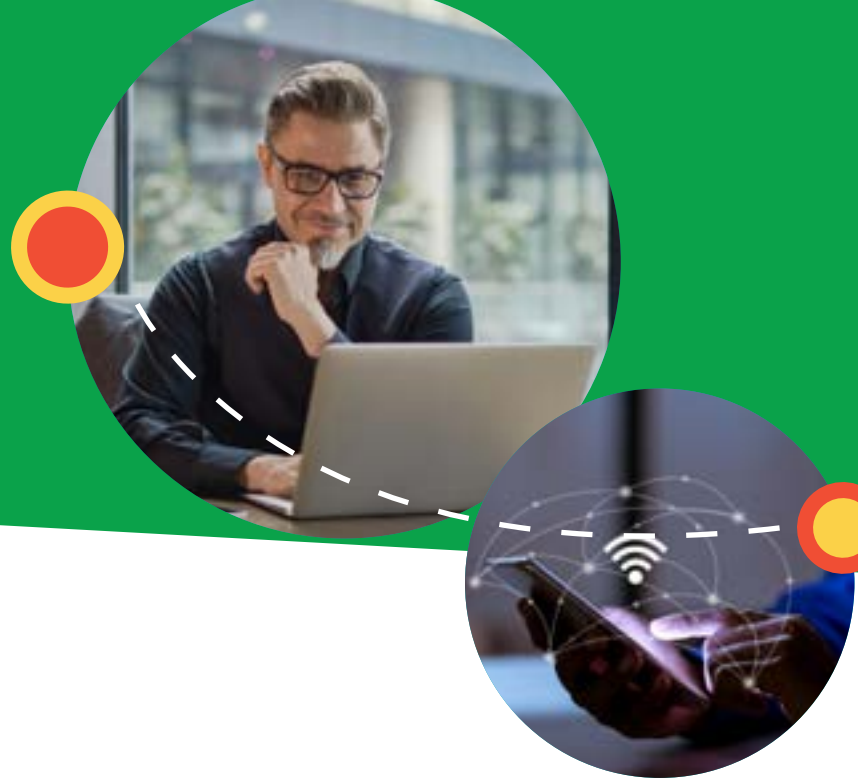
Public Wi-Fi network

Your business's devices and the information on them are particularly vulnerable when working away from the office or home. Many hotels, coffee shops, conference centres and other public places offer Wi-Fi, often for free. This is convenient, but rarely secure.

Avoid open, free Wi-Fi connections unless they are secured with a password and encryption. Even then, use caution when sending your sensitive information. If an unencrypted Wi-Fi connection must be used, business documents and emails should not be transmitted unless a business VPN is used. The VPN will encrypt the transmitted information.

For more details on making these changes, consult Get Cyber Safe's infographic **Is your network ready for anything?**

Virtual private network (VPN)

A VPN can help secure your company's information between your devices and the internet. This is also quite helpful in securing data being used on remote devices and systems. The connected nature of our home lives has made remote work possible, but not every home network is as secure as a business network needs it to be. If you and your employees telework, regardless of the location, protect your business's data and network by using a VPN. Connecting to an unsecured or open network through a VPN adds a layer of encryption to protect the confidentiality of your information. VPNs can come in the form of browser extensions, device apps or as part of your router. Do some research to find out which type of VPN is best suited for your needs.

Anti-virus software

Anti-virus software scans files, emails and downloads before they reach your device. This can help protect your device from malware. Consider choosing software that identifies potentially malicious websites, while also monitoring and flagging suspicious programs. This can protect you from new or unknown malware signatures. While there are lots of free versions of anti-virus software available online, it may be worth investing in reputable paid software for your business. Set anti-virus software to perform regular scans, including during off-hours. Anti-virus software can eliminate known threats and will help keep your devices and your network safe.

For further information, consult Get Cyber Safe's **How to evaluate anti-virus software**.

Firewall

A firewall is a security barrier that can help protect your network, devices and data by blocking unwanted traffic and malicious software. Many operating systems come with built-in software firewalls. If this is not the case, do your research and buy firewall software from a reputable company. For additional protection, you can use a hardware firewall such as one that is built into a router. Check your router's manufacturer resources online to learn how to configure its firewall settings.

You may also qualify for a free domain name system (DNS) firewall service depending on the size of your business, from CIRA Canadian Shield, that provides online privacy and security.

For more information, consult Get Cyber Safe's **CIRA Canadian Shield: Donning your cyber security armour**.

Back to table of contents

4
DEVELOP A BACKUP SYSTEM

Having backups of all data is essential as it ensures that you can recover quickly from damage or loss of data due to accident, natural disaster or a cyber attack. In the case of a ransomware attack, where your company data and systems are locked until a ransom is paid, your backup can save your company from loss of data and money. Your data should be backed up to more than one system to ensure your data is well secured and easy to recover. Here are some examples of common options for storing backups:

> **Cloud storage** saves your files, documents and photos to a remote database. A cloud storage service may come standard with your computer or device. For a business, however, it is often worthwhile to invest in extra storage capacity. Some cloud services may also offer historical file recovery or ransomware protection.

> **External hard drives** are devices that can be connected to your computer or device to save a copy of files, documents and photos. Connect your external hard drive regularly to back up files.

> **External storage** can also be done on network-attached storage (NAS) devices, or a USB key.

Tip

Keep in mind that the best **backup** has its own backup. Even if you use a cloud service, back up your most important data to a secondary external storage device.

Protect your backup system with strong passwords and encryption. When not in use, store external devices in locations that are safe from the elements and unauthorized access. Remember to disconnect external storage devices when the backup is complete. Set backups to take place automatically or set reminders for yourself to back up to external devices at least weekly. Test your backup methods on a regular basis to ensure the backups work for a smooth recovery. Having a smooth recovery is important to ensure your company can function securely and without business delays around unexpected incidents.

Back to table of contents

5

PROTECT CUSTOMER AND SENSITIVE DATA
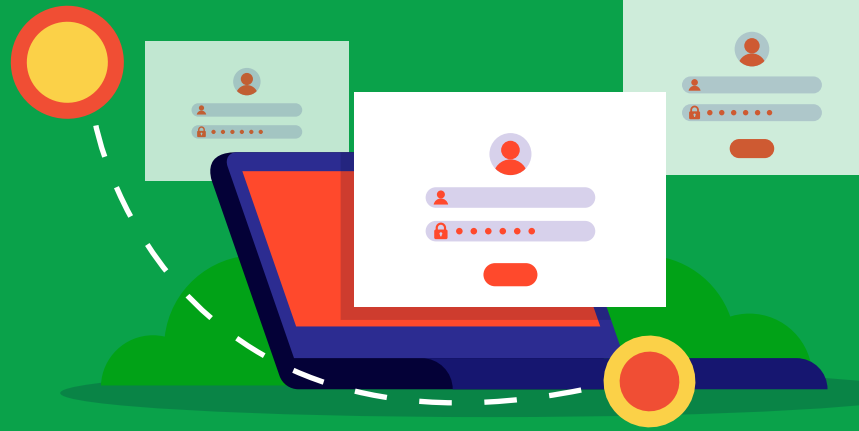
A breach in your cyber security systems could mean the loss of your customers' information. That could cost your business the trust and reputation that you've worked to build up. Customer and sensitive data could include:

> customer data (e.g., names, addresses, payment information)

> financial data (e.g., bank account, tax information)

> employee data (e.g., names, addresses, payroll information)

> propriety data relating to your competitive advantage (e.g., pricing and margins)

This customer and sensitive data may be saved on online databases and or saved on your backup devices. Make sure that wherever this sensitive data is stored, it is encrypted and secured with a strong password. If you use a web hosting service or e-commerce platform, select the highest security level you can afford.

Use a secure e-commerce platform

If you are selling goods online or taking payments online, it is likely you are using an e-commerce platform to do so. There are many e-commerce platforms with built in cyber security solutions that can protect your business from cyber threats.

If you're looking for a new e-commerce platform, research the various security features and options that are offered. This could include things like MFA, customer data encryption, real time threat alerts and compliance features.

If you already have an e-commerce platform, you might want to re-evaluate the features it offers.

And, as always, be sure to update any software you're using. Out-of-date software can have security vulnerabilities that may give cyber criminals a backdoor into your online store.

Back to table of contents

6

ENABLE AUTOMATIC UPDATES

To protect your devices from cyber threats, update your device operating systems and applications regularly and install security patches. Updates and patches don't just fix bugs and improve usability and performance; they often contain components that are very important for protecting your business's security with improvements based on recent viruses and cyber attacks. If you don't update your operating system and software regularly, cyber criminals can use the vulnerabilities to compromise your device, accounts and data.

You can enable your devices and software to update automatically or set updates for a time when systems aren't as actively used, such as overnight. If automatic updates aren't available, install updates as soon as you are prompted.

Back to table of contents

7

DEVELOP A CYBER SECURITY PLAN

Every business should have a cyber security plan. The plan should have detailed procedures for day-to-day operations and ideally an incident response plan (**see step 9 for establishing an incident response plan**). If your business has plans for how to handle everything from a cyber security perspective, your operation will be much more secure.

A cyber security plan sets out the rules a business's employees need to follow. This should include information on software they are allowed to download, how to spot a phishing email and individual roles and responsibilities on what business information they can share online.

A cyber security plan will empower you and employees to help keep your business cyber secure. It will help guide employees whenever they have a question or concern about cyber security.

The cyber security plan should be kept up to date with the latest cyber threats and information.

Cyber security policies should be customized for each individual business. That said, there will likely be common elements that most policies will want to account for. This includes internet usage, email safety and social media.

Canadian businesses are taking more cyber precautions

In 2021, 26% of Canadian businesses had written policies in place related to cyber security, an increase of at least four percentage points since 2019.

https://www150.statcan.gc.ca/n1/pub/22-20-0001/222000012023001-eng.htm

Establish an internet usage policy

An internet usage policy sets out important information about what employees can do online using company devices. In most cases, this includes:

- ☐ Restrictions on the types of websites that employees are allowed to visit
- ☐ Guidelines on what kinds of software they can download as well as requirements for seeking permission to download new programs
- ☐ Requirements to use passphrases or complex passwords for all devices and accounts
- ☐ Expectations when it comes to software updates

Establish a social media policy

Social media is no longer optional for most businesses – it's essential. That leaves more businesses vulnerable to threats from cyber criminals through social media than ever before. Here's what you can provide guidance on for a social media policy:

- ☐ Set rules on what business information can be shared online and where it can be shared
- ☐ Prohibit employees from posting confidential and proprietary information
- ☐ Create instructions on whether employees should use their work email to sign up for social media sites and newsletters
- ☐ Set guidelines on the correct usage of company trademarks

Establish rules for email and messaging safety

Many cyber criminals use email and messaging as a key tactic to steal information from their victims. Some rules and awareness measures should include:

- ☐ Caution employees to be wary of opening and responding to suspicious emails and direct messages
- ☐ Direct employees to avoid opening attachments unless they're from trusted contacts and organizations
- ☐ Restrict the number of personal emails sent using employees' work accounts to limit your business' exposure to online threats that come through personal contacts
- ☐ Specify when it's appropriate for employees to share their work email addresses and limit it to trusted contacts and organizations
- ☐ Tell staff to avoid using the "@" symbol when posting a company email address online (use formatting such as "john at companyxyz dot com" so spambots can't extract the email address)

Establish a bring your own device (BYOD) and telework plan

Decide how (and if) employees should access business data on personal devices and the procedure to follow if a device is lost or stolen. If an employee leaves the business, be sure to remove their access to your accounts.

Template

You can find a cyber security plan template **at the end of this guide.**

8

TRAIN EMPLOYEES

Cyber security is a team effort. One employee's mistake could lead to a virus being installed on a work device and infecting your entire system. It's important to establish cyber security as a fundamental part of your business so that employees understand their impact on cyber security from a personal and business standpoint.

Communicating your business's cyber security plan

By letting employees know what is and isn't cyber secure, you can help educate them on how they can protect your business from cyber threats. Share your cyber security plan with employees and explain the rationale for why it is in place. An informed workforce can defend against cyber incidents as cyber criminals often rely on vulnerabilities related to human error.

Being cyber safe involves individual action, like staying alert and watching out for scams. Scams, such as **phishing or spear phishing**, often specifically target businesses. Everyone in your business should know the **red flags to watch out for,** and follow your company's email and messaging safety plan.

Onboarding new employees should include an introduction to your company's cyber security plan as well.

Awareness and training

Develop training and awareness programs for your employees about cyber security. Create challenges or activities that get everyone involved. For example, see what department can report the most scam emails in a month. When employees are actively engaged and diligent in their personal cyber security, it reflects in the overall business security as well.

Share information about new threats whenever you become aware of them and encourage your employees to report anything suspicious to you, your management or IT team. Once you have an incident response plan in place (**see step 9 to establish an incident response plan**), run your employees through an incident response test to get familiar with the plan and ensure each party understands their part in recovery.

Back to table of contents

Cyber security training course for small businesses

The Cyber Centre's Learning Hub offers a free, self-paced online course for anyone looking to improve their organization's cyber security posture.

Cyber Security for Small and Medium Organizations (course code 625) is designed for learners with minimal technical knowledge and will help you protect your business by walking you through how to implement essential cybersecurity practices and controls.
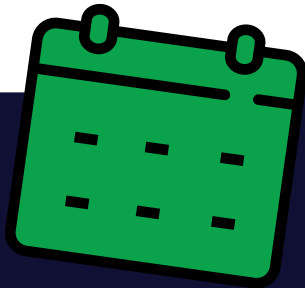
Cyber Security Awareness Month

October is Cyber Security Awareness Month (Cyber Month) and a good occasion to talk about cyber security and hold training sessions. Visit **GetCyberSafe.ca/CyberMonth** for materials you can use to promote cyber security in your business.

Back to table of contents

9
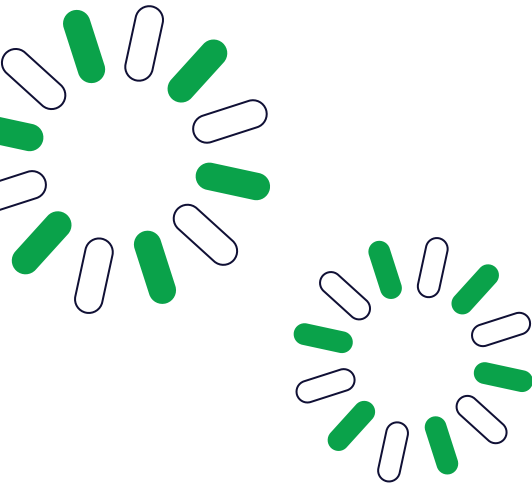
ESTABLISH AN INCIDENT RESPONSE PLAN

You can do everything right for your business and something may still go wrong. If you prepare for the worst, you'll be ready when something unexpected occurs.

An incident response plan includes the processes and procedures to follow to detect, respond and recover from a cyber incident. The following steps should be considered when creating your incident response plan:

Detect

In the detect section of your incident response plan, identify details on:

- [ ] who and what systems monitor devices and data
- [ ] how and to whom employees should report a cyber security issue or concern
- [ ] the internal and external partners you will notify during an incident (e.g., suppliers, investors)
- [ ] reputable professional services that you could contract for help with the cyber incident
- [ ] how you might communicate the incident publicly to preserve your business's reputation and make users aware of potential outages

Respond

In the respond section of your incident response plan, include details on:

- [ ] disconnecting all devices from your network as soon as possible (refer to your asset inventory list created in **step 1**)
- [ ] suspending employee access temporarily to detect and stop further intrusions
- [ ] seeking professional services to resolve the issue, if necessary
- [ ] changing any affected passwords and enabling MFA
- [ ] changing passwords that might also have been compromised through the attack, especially those for administrative accounts
- [ ] contacting your financial institution if financial information was involved
- [ ] reporting the details of the attack to your local police department
- [ ] reporting the attack to the Canadian Anti-Fraud Centre and Canadian Centre for Cyber Security to help protect your business and other businesses from the same attack in the future

Back to table of contents

Recover

In the recover section of your incident response plan, include information on:

- [ ] restoring your systems from a backup
- [ ] updating all software, including your anti-virus software, firewall and firmware once your systems are up and running
- [ ] running anti-malware and anti-virus software on all systems and connected devices
- [ ] patching and updating devices if your run into vulnerabilities
- [ ] identifying any flaws in your cyber security approach that led to the attack

For more details on establishing an incident response plan, refer to the Cyber Centre's publication **Developing your incident response plan (ITSAP.40.003)**.

Template

You can find an incident response plan template **at the end of this guide.**

Test your plan

Testing your response plan will be very helpful. You can identify inconsistencies and address areas that need revision. Here are four different approaches to testing your response plan:

- [ ] **Checklist:** Read through and explain the steps of the response plan. Address all assets and systems that need to be considered if a cyber attack occurs.
- [ ] **Walkthrough:** Walk through the individual components in the response plan to find vulnerabilities where further security tools could be used when considering specific incidents or disasters.
- [ ] **Simulation:** Perform a simulation of the response plan by using a simulated incident. Simulation testing will help familiarize your team with their roles and responsibilities and assess how well the response plan functions.
- [ ] **System tests:** Set up and test backup systems to see if they can perform operations and support key processes. Test your backup systems by partially and fully disconnecting your main systems to ensure business processes can continue if systems are compromised.

Testing your systems help assess the limitations you may experience during a cyber attack. It is important to test how your systems can best support your operations while disruptions occur to have a smooth recovery process.

Back to table of contents

10

STAY UP TO DATE

The cyber threat landscape is evolving with new vulnerabilities and new tactics being discovered.

You can keep your organization up to date and aware of current cyber threats by keeping up with news, alerts and resources provided by the Get Cyber Safe public awareness campaign and the Canadian Centre for Cyber Security.

> Follow **cybercentre_ca** on X for the latest cyber alerts and advisories

> Visit the Canadian Centre for Cyber Security website **Cyber.gc.ca** for expert advice, guidance, services and support on cyber security for Canadians

> Visit the Get Cyber Safe website **GetCyberSafe.ca** for simple steps you can take to protect yourself online and resources to hold Cyber Month in your organization

> Share your knowledge and these resources with your suppliers, vendors and customers to help secure your entire supply chain

Back to table of contents

CONCLUSION

With a surge of business operations taking place online, cyber security is increasingly important for small businesses. By focusing on getting cyber safe in your business operations and following the steps laid out in this guide, you can help defend your business against cyber threats of all kinds.

For more information and templates, visit **GetCyberSafe.ca/business**

CYBER SECURITY PLAN

Company name:

This cyber security plan describes how we will keep our business cyber secure.
It will help guide us whenever we have a question or concern about cyber security.

Last updated this cyber security plan on	
The person responsible for cyber security at is:	

Responsibilities include:

- consulting the Get Cyber Safe SMB Guide
- planning, implementing and maintaining this plan
- helping other staff understand cyber security best practices and policies

INTERNET USAGE POLICY

Employees of :

- use complex passwords and enable multi-factor authentication (MFA) whenever available
- enable automatic updates or install updates whenever they become available
- consult before downloading new software on company-owned devices
- do not use company-owned devices to commit any kind of illegal activity, including piracy of music, movies and other content

EMAIL AND MESSAGING SAFETY

Employees of :

- are familiar with the **7 signs of phishing**
- are cautious when opening suspicious emails and messages
- do not open suspicious attachments
- flag any suspicious activity to
- share their work email addresses only with trusted contacts and organizations
- avoid using the "@" symbol when posting a company email address online — instead, use formatting such as "john at companyxyz dot com"

SOCIAL MEDIA POLICY

Employees of :

- use their personal (not company) email addresses to sign up for personal social media accounts and newsletters
- do not share confidential or sensitive company information on social media
- seek permission before posting or responding on social media on behalf of
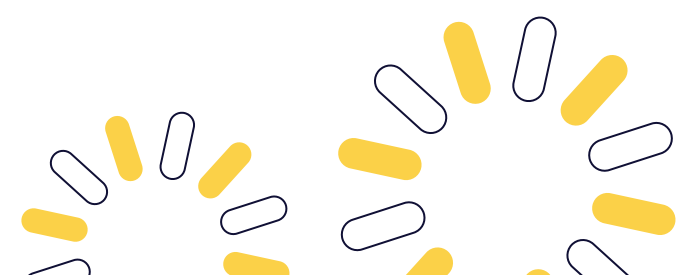
BRING YOUR OWN DEVICE (BYOD) PLAN

Employees of _____ using their own devices for company business:

- must keep their personal device updated with a recent operating system (OS) and enable automatic updates
- may not use a personal device that has been jail broken (iOS), rooted (Android), or otherwise compromised
- can only download applications from trusted sources such as the device's app store
- must set their device to lock automatically and unlock it with a PIN, password or biometric
- must not access sensitive company information using their personal device
- should know who to contact (and have the correct contact information) if they experience security issues or their devices are lost or stolen
- must wipe all personal and company information before returning or disposing of a personal device

EMPLOYEE DEPARTURE PLAN

When an employee is leaving

- business property such as laptops, keys and access badges must be promptly returned
- access to company accounts must be removed

ASSET INVENTORY LIST

Asset suggestions:

- desktop computer
- laptop
- router

- mobile phone
- tablet
- printer

- scanner
- monitor
- keyboard

Asset type	Asset name	Serial number	Location	Owner and contact info	Notes (e.g. software license expiry date)

INCIDENT RESPONSE PLAN

An incident response plan includes the processes and procedures to follow to detect, respond and recover from a cyber incident.

DETECT

The cyber security lead is responsible for monitoring company systems and data for cyber incidents. Employees should report any security issues or concerns to the cyber security lead.

The cyber security lead for _____ is:	Contact info:
	Alternative contact info:

KEY CONTACTS:

In the case of a cyber security incident at _____ , the cyber security lead will inform:

_____'s Communications lead:	Name:
	Contact info:

Depending on the details of the incident, the cyber security lead will also inform:

_____'s Legal lead:	Name:
	Contact info:
_____'s Key suppliers:	Name:
	Contact info:
_____'s Key clients:	Name:
	Contact info:
_____'s Investors:	Name:
	Contact info:

Depending on the severity of the incident, the cyber security lead will enlist the services of a professional computer services provider:

Name of provider:
Contact info:

Identify how you might communicate the incident publicly to preserve your business' reputation and make users aware of potential outages.
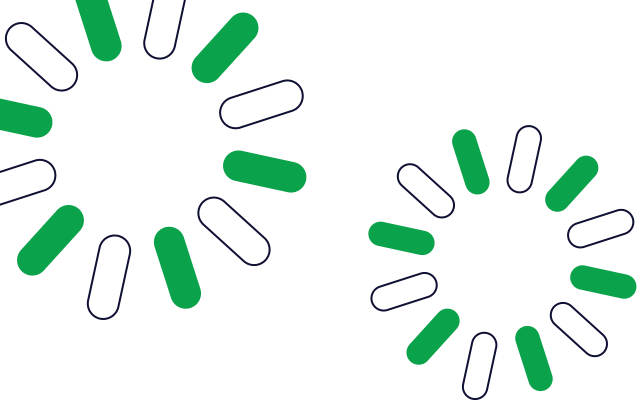
RESPOND

Steps to take to respond to a cyber incident:

1 Disconnect all devices from your network as soon as possible (refer to your asset inventory list)

2 Suspend employee access temporarily to detect and stop further intrusions

3 Seek professional services to resolve the issue, if necessary

4 Change any affected passwords and enable multi-factor authentication (MFA)

5 Change additional passwords that might also have been compromised through the attack, especially those for administrative accounts

6 Communicate the incident publicly with a statement such as:

> We experienced a cyber security incident [earlier today] and we are working [with cyber security experts] to resolve the situation. We sincerely apologize for any inconvenience this may create for our valuable customers.
> Our priority is to resolve this issue [and provide information to those affected] as soon as we can.

7 Contact your financial institution if financial information was involved

8 Report the details of the attack to your local police department

9 Report the attack to the **Canadian Anti-Fraud Centre** and **Canadian Centre for Cyber Security** to help protect your business and other businesses from the same attack in the future

RECOVER

Steps to take to recover from a cyber incident:

1 Restore your systems from your backup

2 Update all software, including your anti-virus software, firewall and firmware once your systems are up and running

3 Run anti-malware and anti-virus software on all systems and connected devices

4 Update devices

5 Identify any flaws in your cyber security approach that led to the incident