For the full version of Get Cyber Safe's Guide to Cyber Security for Small Business, **visit GetCyberSafe.ca/business**

GET CYBER SAFE'S QUICK GUIDE TO CYBER SECURITY FOR SMALL BUSINESS

Start protecting your business from cyber threats right now with this quick guide. By following the ten steps listed below, you will be well on your way to securing your business against common cyber threats.

1. TAKE STOCK

Make a list of all the internet-connected devices and assets your business uses. This list may include:

- desktop and mobile devices (computers, laptops, tablets and phones)
- storage devices (hard drives and USB keys)
- peripherals (printers, scanners, monitors, keyboards, mouses and docking stations)
- internet-connected devices (point-of-sale (POS) devices, smart security systems and smart speakers)
- digital assets and services (social media accounts, websites, cloud and online bookkeeping services)

Take note of the location of each item, and who has the login and password to access to it.

2. SECURE YOUR DEVICES

Secure each of your business's devices with a **strong passphrase or password** that's unique to each device. Be sure to update passphrases on devices that came with a default password such as routers and Bluetooth devices. **Activate multi-factor authentication (MFA)** wherever possible. Limit who has administrator privileges, ensuring that access is granted exclusively on a need-to-know basis.

GETCYBERSAFE.CA

Canada

3. SECURE YOUR NETWORK

Your business's network is the gateway to all your connected devices. Protect it with a **firewall** that monitors network traffic and filters out malicious sources. You can also install **CIRA Canadian Shield**, a free DNS firewall service that provides online privacy and security.

Next, choose the best **anti-virus software** for your business. Ensure that it scans for known malware and removes it, protects your devices from malicious websites, and monitors and flags suspicious program behaviour. If your employees telework, provide them with a **virtual private network** (VPN) so that they can connect securely from wherever they are working.

4. DEVELOP A BACKUP SYSTEM

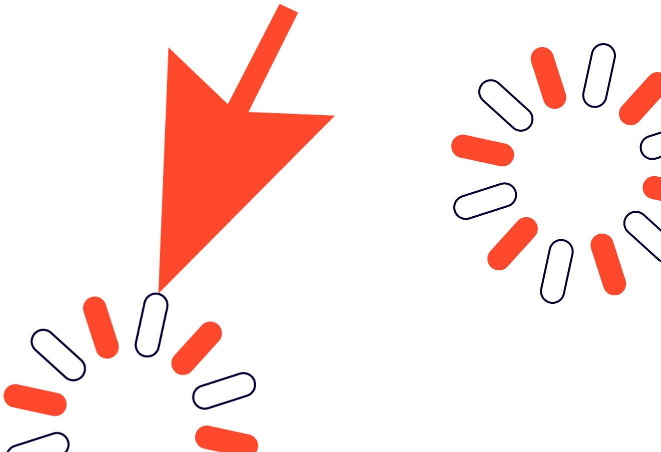
Having backups of all data is essential, as it ensures that your business can recover quickly from loss of data due to a cyber attack. If you choose to back up using a **cloud service**, review the privacy policies and security features offered by your cloud provider, and use a strong passphrase. Keep 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 storage device, such as an external hard drive or USB key. Determine how often you'll perform backups or set devices to back up automatically, at least weekly.

5. PROTECT CLIENT AND SENSITIVE BUSINESS 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. Always protect sensitive business data with strong passphrases. If your business uses an e-commerce platform, make sure it includes security features like MFA, data encryption, real-time threat alerts and compliance features.

6. ENABLE AUTOMATIC UPDATES

Operating system (OS) and software **updates** often contain components that are very important for protecting your business's security with improvements based on recent viruses and cyber attacks. Enable updates to install automatically for operating systems and for software. If automatic updates aren't available, install updates as soon as you are prompted.



7. DEVELOP A CYBER SECURITY PLAN

A **cyber security plan** sets out the rules you and your employees need to follow. This may include:

- requirements to use passphrases and MFA on business devices and accounts
- rules on the websites employees may visit and the software they may download
- advice on email safety, including how to avoid **phishing scams**
- guidelines on accessing business data on personal devices
- a social media plan outlining what can be shared on the business's social media accounts
- procedures for employee departures such as revoking accesses and changing passwords

8. TRAIN EMPLOYEES

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. Schedule training sessions regularly to refresh your employees' memories and to ensure new employees benefit from this training. October is Cyber Security Awareness Month and a good occasion to talk about cyber security.

9. ESTABLISH AN INCIDENT RESPONSE PLAN

An incident response plan outlines how your business will detect, respond to and recover from a cyber incident. Your plan should include elements such as:

DETECT > procedures for employees to report issues

RESPOND > procedures for isolating the affected device or system, and procedures (possibly including professional services) for resolving the issue

RECOVER > procedures for restoring your systems from your backup

10. STAY UP TO DATE ON CYBER SECURITY

Additional information on each of these steps is available in the full Guide to Cyber Security for Small Business and on **GetCyberSafe.ca/business**. For more in depth information on cyber threats and mitigation strategies, visit the **Canadian Centre for Cyber Security**. And, for the latest advice and guidance, follow the Cyber Centre and Get Cyber Safe on social media.

@GetCyberSafe

GETCYBERSAFE.CA

Catalogue number: D96-87/2022E-PDF | ISBN: 978-0-660-43025-6

Canada