GETCYBERSAFE

Protect while you connect.

## Know the Risks.

## Protect Yourself.

## Protect Your Business.

# GETCYBERSAFE TIPS FOR SMALL AND MEDIUM BUSINESSES

Canada

GETCYBERSAFE
Protect while you connect.

## If you're like most small or medium businesses in Canada, the Internet is an indispensable tool for succeeding in today's digital world.

Whether you have a website or not, you probably still use the Internet for everyday tasks like email, banking, and ordering supplies.

But, the more you use the Internet for your business, the more problems you can run into.

That's why we have gathered some tips to help you improve your business's cyber security plan, so you can stay safe from hacking and data theft, among other things.

For a more in-depth and instructional look, or if you would like to take the cyber security self-assessment, download our Small and Medium Business Guide at **GetCyberSafe.gc.ca**.


Cat. No.: PS4-186/2013E-PDF
ISBN: 978-1-100-22866-2

Canada

# Management Issues

***A good cyber security plan starts at the top — which, if you're reading this, is probably you. Here are some steps you should take to kick your plan off properly:***

1. Develop and implement a cyber security plan that clearly outlines best practices for all employees.

2. Assign at least one person to be responsible for your business's cyber security, and make sure to give them clear instructions on what you expect from them.

3. Determine what risks to your business are low-, medium-, or high-level threats – this will help you prioritize.

4. If you have any legal concerns about cyber security, don't hesitate to consult with experts (i.e., legal counsel).

5. Explain policies and standards to employees so that they will understand why you need them in place, to whom they apply, why they're important, and the risks to themselves or the company if they don't follow them.

6. It's easy to underestimate how much a cyber security plan can cost, so make sure to budget properly.

# Web Security

***It's simple: your business has access to the Internet because employees need it for work (and for a bit of downtime, too). Either way, they're using it. Here are a number of things you can do as part of your cyber security program to make sure their browsing doesn't hurt them or your business:***

1. Restrict the types of websites that employees are allowed to visit – this can help you exclude the sites that could compromise your network.
2. Advise employees on what software is safe to install on their computers, and to seek permission when downloading new programs.
3. Write an Internet Usage Policy for personnel to follow and post it in an accessible place for all to see and refer to. This should set rules for what kinds of information your employees can share online.
4. Update all of your business software when you receive notifications to do so, so that all security fixes are up to date.
5. Require all of your employees to have complex passwords that have letters, numbers and symbols so they are harder for cyber criminals to steal.
6. Always be suspicious of phone calls, emails or other communications from an unknown source.

GETCYBERSAFE
Protect while you connect.

Canada

# Point-of-Sale (POS) Security

*Your business's point-of-sale (POS) system requires an Internet connection to process transactions – which is pretty much a requirement if you want happy customers. But with anything that needs an Internet connection comes security risks as well. Here are some ways you can help make sure that cyber criminals don't use your POS system for malicious purposes:*

1. Do not use the default username and password provided by the manufacturer.
2. Make sure your POS system is behind a firewall.
3. Set up strong encryption for all transmitted data (note: the service provider should implement this by default).
4. Limit access to client data to those employees who absolutely need it.
5. Ensure that all anti-malware software is up to date, as new security updates are introduced frequently to fight new types of malware.
6. If you have any concerns with the security of your POS system, contact the POS service provider.

GETCYBERSAFE
Protect while you connect.

Canada

# Email Security

***Email is a requirement for any business in today's world. Getting a lot of emails usually means good things for your business, but spam and phishing scams can make email dangerous. Here are some tips to help make it less dangerous:***

1. Implement a spam filter — doing so will help you get rid of most potentially harmful emails sent by cyber criminals. Also, never forward those emails to others.

2. Don't click on any unverified or suspicious links — even just clicking a link could give away sensitive information that a cyber criminal can use to hurt you and your business.

3. Keep your employee and customer emails and information confidential, as this information can be used to hurt employees or your business.

4. Enable HTTPS for Web-based email, which encrypts data and essentially makes it impossible for cyber criminals to access the information in your browser.

5. Set strict password standards for all email accounts being used at work (business or personal).

6. When possible, use generic emails – for example, info@companyname.com – for email addresses that are posted in public places (such as on your website or on social media).

GETCYBERSAFE
Protect while you connect.

Canada

# Data Security Tips

***Data is the backbone of your business – without it, you have nothing. Simply, it is an important thing to protect. Here are some ways you can do that:***

1. Frequently back up your data to an external hard drive, server and/or online service — having multiple backups of your data is key in case of the failure of one of them.
2. Download or purchase automatic backup software to ensure regularly scheduled backups of your system(s).
3. Store your physical backups (e.g., external hard drive) offsite in a safe place.
4. Prepare emergency system boot DVDs or USB sticks in case of a system crash.
5. Properly label any sensitive information you have to ensure secure handling.
6. When disposing of your data, thoroughly destroy it — shred all paper and CDs — so that no information could potentially be gathered and used to harm you.

GETCYBERSAFE
Protect while you connect.

Canada

# Remote Access Security

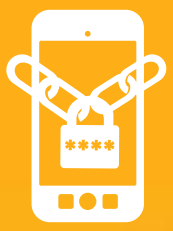
*Remote access allows you and your employees to connect to your business network from anywhere in the world. Awesome, right? While it is handy, it also opens up your business to security risks that could hurt it. Here are some ways to avoid that:*

1. Conduct your remote computing through a Virtual Private Network (VPN).
2. Limit access to your network to authorized personnel with a clear business need.
3. When working from home, properly secure your Wi-Fi before using your VPN.
4. Do not use unknown or unfamiliar Wi-Fi connections when travelling.

GETCYBERSAFE
Protect while you connect.

Canada

# Mobile Device Security



***Mobile devices and portable data storage (such as USB sticks) allow your business to be more productive and make communication easier. However, the data they contain could be used to hurt your business. Here are some ways you can ensure proper mobile device security:***

1. Ensure that all of your mobile business devices (phones, tablets) have system access passwords and are locked when not in use.

2. Properly safeguard data on mobile devices by using the built-in security features or installing anti-malware software.

3. Encrypt all of your sensitive data on portable storage devices.

4. Make sure that you apply the Web Security and Email Security tips to your mobile device habits.

GETCYBERSAFE
Protect while you connect.

Canada

# Physical Security

***Your business's security is only as good as the people that have access to it. You may have already thought of protecting your business systems against visitors and former employees, but there are some other things you can do to make sure that your business is secure:***

1. Only give your employees access to what they need access to.
2. Have your employees lock their computers and put away sensitive documents when not at their desk.
3. Create and enforce an employee security policy.

GETCYBERSAFE
Protect while you connect.

Canada