GETCYBERSAFE

Protect while you connect.

Know the Risks.

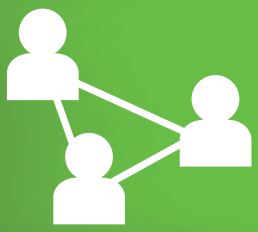
Protect Yourself.

Protect Your Business.

GETCYBERSAFE GUIDE FOR SMALL AND MEDIUM BUSINESSES

Canada

Table of Contents



Introduction

If you're like most small or medium businesses in Canada, the Internet is an indispensable tool to succeed in today's digital economy. Getting online allows you to reach new customers and grow your business. And even if you don't have a website — or a Facebook page or Twitter account — you probably depend on the Internet for everyday business operations like banking, payroll or ordering supplies.

However, being online requires being safe and secure. As a small or medium business, it's easy to think that you are too small to warrant the attention of cyber criminals. In fact, cyber criminals are now actively targeting smaller businesses because they believe their computers are vulnerable.

This guide is designed to help Canadians who own or manage a small or medium business understand the cyber security risks they face, and provide them with practical advice on how to better protect their business and employees from cyber crime.

In other words, if you are a small or medium business owner, this guide is for you. Cyber security is a shared responsibility and, depending on how your business is structured, there are likely other people — co-owners, managers or employees — who should also be familiar with the information you'll find in this guide.

You do not need to be a computer or Web expert to read or implement the measures in this guide. Although some cyber security terms are used, you can look up any terms you are unfamiliar with in the glossary at the end of this guide or online in the GetCyberSafe.ca glossary.

The self-assessment tool in Appendix A can help you determine where your business needs the most help.

If you are experiencing a serious cyber incident, contact the police, seek professional assistance and consult Appendix C of this guide for additional resources.

Cyber crime and smaller businesses

- Small and medium-sized businesses (i.e., businesses with fewer than 500 employees) employed 10 million people in 2012, nearly 90% of all employees in Canada.[1]
- In 2012, 87% of Canadian businesses used the Internet, and 46% had a website.[2]
- The largest growth area for targeted cyber attacks in 2012 was businesses with fewer than 250 employees — 31% of all attacks targeted them.[3]
- Over a 12-month period in 2012, 69% of Canadian businesses surveyed reported some kind of cyber attack, costing them approximately $5.3 million, or about $15,000 per attack.[4]

[1] Source: Key Small Business Statistics - August 2013, Industry Canada, http://www.ic.gc.ca/eic/site/061.nsf/eng/02805.html
[2] http://www.statcan.gc.ca/daily-quotidien/130612/dq130612a-eng.htm
[3] Symantec 2013 Internet Security Threat Report http://www.symantec.com/security_response/publications/threatreport.jsp
[4] ICSPA report: Study of the Impact of Cyber Crime on Businesses in Canada, https://www.icspa.org/fileadmin/user_upload/Downloads/ICSPA_Canada_Cyber_Crime_Study_May_2013.pdf

Cyber Security Fundamentals

Cyber security is about protecting your information, which is often the most critical and valuable asset a business will own. Cyber security is based on three fundamental goals:

- *Confidentiality*: Any important information you have — such as employee, client or financial records — should be kept *confidential*. This information should only be accessed by people (or systems) that you have given permission to do so.
- *Integrity:* You need to make sure to maintain the *integrity* of this information and other assets (such as software) in order to keep everything complete, intact and uncorrupted.
- *Availability:* You should maintain the *availability* of systems (such as networks), services and information when required by the business or its clients.

Achieving and maintaining these goals is an ongoing process. Good cyber security involves the following:

1. Determining what assets you need to secure (essentially, anything of value managed or owned by your business).
2. Identifying the *threats* and *risks* that could affect those assets or your business overall.
3. Identifying what *safeguards* you should put in place to deal with threats and secure assets.
4. Monitoring your safeguards and assets to prevent or manage security breaches.
5. Responding to cyber security issues as they occur (such as an attempt to break into business systems).
6. Updating and adjusting to safeguards as needed (in response to changes in assets, threats and risks).

Cyber Security Fundamentals

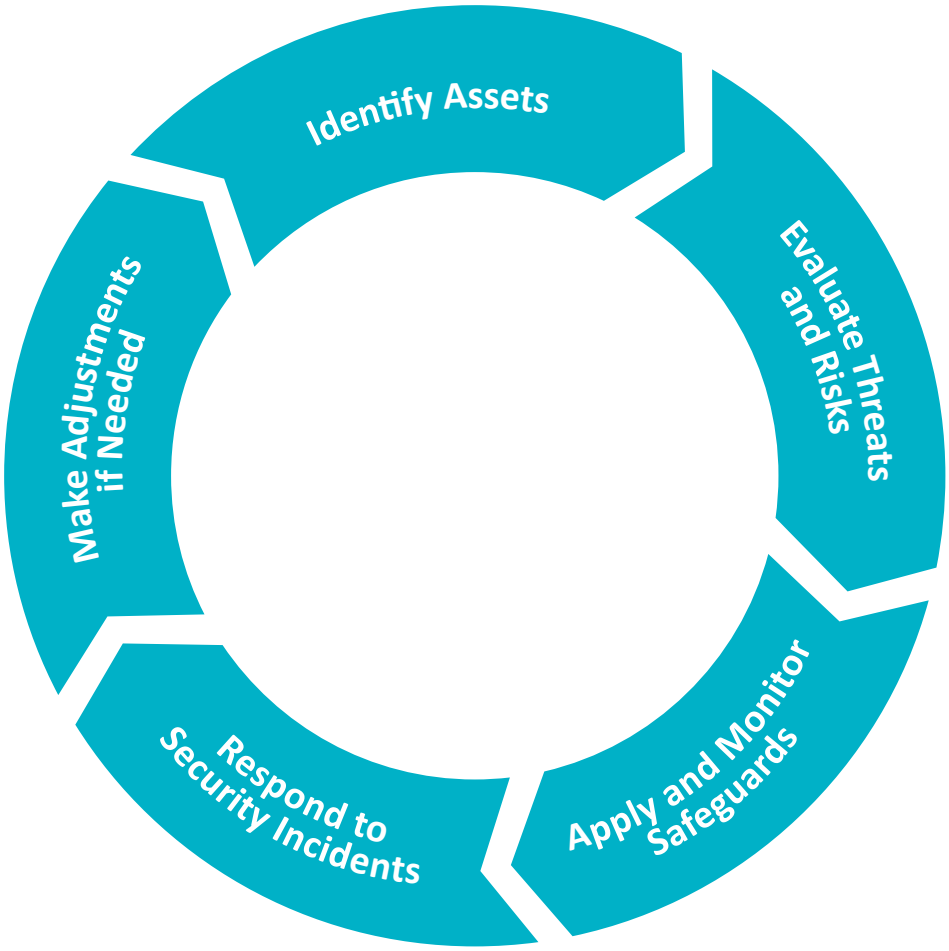


Figure 1

The term *threat* refers to any potential danger to your business, its assets or employees. Threats can be natural, such as fire and flood. They can also be human in origin. In fact, human threats are becoming more common and require a lot of your attention.

The biggest challenge for your business is to define and prioritize assets, threats and the potential risk of those threats. Then, you have to apply appropriate *safeguards*. Safeguards are anything you can use to counter threats and reduce risk. These can be anything from software and hardware to policies and specific procedures (for employees or clients to follow). In many cases, a safeguard is made up of a combination of these elements.

The rest of this guide provides advice on how your business can set up a sound cyber security process, including identifying threats and risk, establishing safeguards and putting in place the management structures you need to keep your protections up to date.

Management Issues

Quick tips from this section:

- Develop and implement a cyber security plan that clearly outlines best practices for all employees.
- 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.
- Determine what risks to your business are low-, medium- or high-level threats — this will help you prioritize.
- Make sure that employees understand why cyber security is important for them and your business.
- If you have any legal concerns about cyber security, don't hesitate to consult with experts (e.g., legal counsel).
- Explain policies and standards to employees so that they will understand why you need them in place, to whom they apply and the risks to themselves or the company if they don't follow them.
- It is easy to underestimate how much a proper cyber security plan can cost, so make sure to budget properly.

3.1 Security Awareness

Trying to keep up with cyber security can seem overwhelming. A good first step is putting in place a security awareness program.

A security awareness program is a way of keeping you and your staff informed about good cyber security practices. It can be very simple and readily developed by you or other employees. It should start with basic training for staff. Over time it should expand to include updates and reminders on policies, standards and best practices. Your security awareness plan can include a regular, scheduled review to update existing security measures for your business, including adopting new means of protection (both software and hardware) as needed.

"A security awareness program very simple and readily developed by you or other employees."

Training and educating personnel is vital to having a strong cyber security system in place. Choose topics that are simple, focused and concise. Key messages should be repeated, but it is important to engage with personnel in multiple ways to avoid having your messages ignored. For example, spam advice could be reinforced through emails, posters and staff meetings. You could even supplement this with periodic quizzes, contests and rewards to keep employees interested and involved.

Management Issues

3.2 Defining Roles and Responsibilities

You should put at least one person in your business in charge of cyber security. This person would be responsible for the following:

- Learning about threats, trends and security options.
- Planning, acquiring and implementing security safeguards.
- Helping other personnel understand cyber security best practices and policies.
- Enforcing cyber security best practices and policies with management support.
- Maintaining and updating the security safeguards used by your business.

Even with a clear person or group in charge of cyber security, their success within a business of any size relies on management support. The support you provide will depend on the size of the business, but some of the things all managers are responsible for include the following:

- Providing guidance to all employees on the importance of cyber security as part of operations, including policies to outline accountability for cyber security.
- Supporting and monitoring cyber security projects.
- Consulting with experts, such as legal counsel, for any external obligations such as provincial or federal law.

3.3 Developing Policies and Standards

The only way employees will know how to conduct themselves is if you put sound cyber security policies and standards in place.

A security *policy* is a document that explains what employees may or may not do with respect to cyber security. Internet use policies, social media policies and acceptable use policies are all examples of security policies. An acceptable use policy might state, "you may not connect a personal computer to the business network," or "when accessing the business network from home, you must use the provided security tools."

Cyber security policies do not need to be long or complicated. But they are essential in helping your employees understand their roles and responsibilities.

A security policy is a document that states what personnel may or may not do with respect to cyber security.

A standard is a document that explains how a specific task should be done. Standards most often apply to setting up and using technical systems.

A *standard* is a document that explains how a specific task should be done. Standards most often apply to setting up and using technical systems. For example, a password standard would describe exactly what an acceptable password can or cannot include, how long it should be and how often it should be changed.

Management Issues

You'll probably want to write your own cyber policies in-house as they need to be specific and may change over time. You will also most likely have certain areas that particularly concern you.

When developing and using cyber security policies and standards in your business, consider the following:

1. Begin with a comprehensive, but relatively simple, cyber security policy to clearly lay out key principles and rules for cyber security within your business.
2. Identify and adapt existing standards to deal with specific cyber security issues or technologies in the business, or write your own.
3. Explain policies and standards to personnel so that they will understand the rationale for rules, to whom they apply and any consequences for not following the policy.
4. After the initial cyber security policy and associated standards are in use, you may wish to revisit those and add more detailed, specific information such as those identified in the various sections of this guide. For example details regarding the use of a social media if your business uses a lot of it or expectations and obligations regarding mobile security if a number of your staff are issued mobile devices.

3.4 Cyber Security Planning

A study in 2012[1] found that 83% of small and medium businesses do not have a cyber security plan in place. Developing a cyber security plan should be a priority for any business. A cyber security plan will identify what assets need to be secured, what threats and risks to focus on, and which safeguards to implement — all in order of priority.

Here are some steps to help you prepare a cyber security plan for your business:

1. Complete the simple Cyber Security Status Self-Assessment Tool in Appendix A of this guide. This will identify gaps and options in cyber security in your business.
2. Identify all business assets (such as computers and business information) and determine their importance and value to the business.
3. Discuss cyber security threats with employees or outside experts (as required) and determine which assets are at risk of harm if one or more of those threats occur.
4. Prioritize risks as high, medium or low.
5. With the help of employees or outside experts, determine what can be done to reduce those risks.
6. Evaluate the threats, risks and potential security safeguards and then decide what can and should be done to improve cyber security in the current year. Often one improvement can be planned in conjunction with another to help reduce overall costs. For example, if you are already setting up a network firewall, there may be options to help deal with malware or spam within the firewall.
7. Set attainable target dates for all identified cyber security tasks and security safeguards that you plan to purchase.

[1] 2012 NCSA/Symantec National Small Business Study.

8. Identify resources that will be needed to implement the plan in the first year including people, time and money.
9. List any issues that may hinder your plan (such as a lack of personnel or budget).
10. Start implementing the plan.
11. Repeat Step 3, threat evaluation, at a minimum of once per year.

Make sure to keep track of any changes in the plan and inform all affected parties (such as vendors) to avoid confusion. For example, if you have hired a security expert to help set up a firewall and find that spam has become a more urgent priority, you may need to adjust your plan either to focus on spam or to incorporate spam blocking within the firewall.

You should also evaluate progress at every year-end and make any necessary adjustments. In most cases, a multi-year cyber security plan will need some updates each year to accommodate changing priorities and business capability.

While the process to develop a cyber security plan may seem daunting at first, remember that you can always revisit and expand your plan over time.

3.5 Budgeting for Cyber Security

Having an effective cyber security plan costs money and must be taken into account when drawing up your annual business plans and budgets. Fortunately, there are some free services, tools and advice available. Additionally, policies or internal documents can often be developed in-house at minimal cost.

But some key things, like security safeguards, will have to be purchased and may also involve annual subscription fees. For example, unlike software that you typically pay a one-time fee for, a subscription to anti-malware software might need to be renewed each year for a fee.

To avoid surprise expenses, it is best to allow for the following:

1. The first-time cost of any security tools, as well as upgrade or update fees.
2. Any support, consulting or training costs.
3. 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 this with your insurance provider in advance.

Web Security

Quick tips from this section:

- Restricting the types of websites that employees are allowed to visit can help you exclude the sites that could compromise your network.
- Advise employees on what software is safe to install on their computers, and to seek permission when downloading new programs.
- When someone outside of your business requests any personal or business information, verify that they are a safe person to send the information to.
- Write an Internet Usage Policy for personnel to follow and post it in an accessible place for all to see and refer to.
- Set rules on what kinds of business information your employees can share online, and where.
- Create instructions on whether your employees should use their work email to sign up for social media sites and newsletters.
- Consider the implementation of a company social media policy, so that employees know what they should and should not post online.
- Update all of your business software when you receive notifications to do so, so that all security fixes are up to date.
- Require all of your employees to have complex passwords that have letters, numbers and symbols so they are harder for cyber criminals to steal.
- Always be suspicious of phone calls, emails or other communications from an unknown source.

4.1 Protecting Personal and Business Information Online

For their own security and the security of your business, employees should protect their personal and business information online. Personal and business information includes private or confidential details like full names, social insurance numbers, email and phone numbers, addresses, banking and other account information and passwords.

It's important that all employees understand why protecting information online is important. Criminals who want to harm or steal from your business often begin by collecting personal or business information in order to gain access to your computer systems and confidential information.

Here are some simple tips for all employees:

- Only visit legitimate and trusted websites while using business computers or working with business information.
- Before providing personal information to anyone, verify that they are a trusted source (for example, a bank would not send out personal inquiries by email, so a call to the actual bank might be advised if such an email were received).

- If someone is seeking your personal information, ask why the information is required.
- If the answer does not seem satisfactory, do not provide it — or ask for their supervisor to get more details.
- Never remove or disable any security safeguards put into place on business networks and computers (such as anti-virus software).

4.2 Browsing the Web Securely

Research, collaboration, communication with clients, purchasing and many other business activities rely on the Internet. However, there are many threats to your business on the Web, starting with those encountered while doing a simple, everyday task: browsing.

Safe browsing involves a combination of security safeguards and practices. Here are some steps you can take to make sure that your business browses safely and securely:

1. Begin by writing and publishing an Internet Usage Policy that clearly explains to employees what they can and cannot do when using business systems to connect to the Internet. Examples of Internet Usage Policies can be found online.
2. Train your employees on the content of your Internet Usage Policy.
3. Encourage ongoing security awareness by regularly communicating with employees about safe browsing practices.
4. Explain to employees how to check the URL of websites they are going to visit to avoid visiting dangerous websites (see the tip box that follows).
5. Implement a site-rating tool as an extension to the browser on user computers (Figure 2). This will help employees identify safe websites.

Figure 2: A Sample Screen from a Site Rating Tool

Web Security

How to identify suspicious links on Web pages

Hovering your cursor over a link will display the actual destination URL either in a small text box that appears temporarily over the link, or at the bottom of the browser window. Try this before clicking on a link and check for the following:

- If the linked text is a URL, compare it with the actual destination. Cyber criminals often use text like "Log in to www.mybank.com to update your account information," but the actual destination is a lookalike site at another location such as www.myfakebank.com.
- Check for URLs that are similar to sites you know, but are slightly different (such as Goggle.com or Google1.com instead of Google.com). This technique is commonly used to trick people into false confidence when visiting sites. In many cases, the fake sites are made to look almost identical to the original it is copying.
- Always be suspicious of URLs you don't recognize.
- Remember that images as well as text can be linked, so use the same caution clicking on images as you would with text.
- When in doubt, copy and paste the URL into a search engine to identify the site without visiting it.

4.3 Social Media

Social networking sites like Facebook, Twitter and LinkedIn can be powerful tools for your business to reach potential customers and build stronger relationships with clients. However, social networking sites and services are becoming an increasingly popular way for cyber criminals to try to get your personal or business information to hack into your personal or business computer systems.

If your business uses social networking sites for marketing or professional purposes, you will need to choose one or more employees, and allow only them to post content in your business's name.

Social networking should be addressed in your business's Internet Usage Policy, with clear advice to employees. Here are some social networking issues that you should consider:

- Be clear on what information about your business can be posted and who is authorized to do so.
- Refrain from including sensitive business information in the business profile or your posts.
- Be careful using applications on social networking sites. Many of these come from third parties and may not be secure. Always check on the application provider first.
- When communicating through social media, be suspicious of any messages that are asking for sensitive business information or about employees and their families.
- Think before you post! What you post to social media sites is generally permanent. You may someday change your mind about what you said online, but you can't remove or change it.

Web Security

While at work, your employees are also likely to use social media for personal reasons, whether to connect with friends and family or keep up with news and events. It is important that employees follow similar guidelines to protect their own information when social networking as well as your business's networks and devices.

Here are some additional tips for employees when using social media for personal purposes:

- Criminals are interested in the information you post. To help your business stay safe, make sure you use the site's privacy controls and ignore requests from people you don't know.
- Review and stay up to date with the social networking site's privacy policies (most are updated frequently) and adjust personal privacy settings appropriately.
- Never reveal your precise location online.

4.4 Social Engineering

Social engineering is when a cyber criminal manipulates someone in order to obtain information about a business or its computer systems.

Cyber criminals use social engineering to gather the information they need to commit fraud or gain access to computer systems. They will seem earnest and respectable. They may even tell you that they have a legitimate connection to your business (for example, as a client or through another business) and offer "proof." Some will impersonate the government. They will often ask for information such as phone numbers or account information, or ask that you open emails with attachments or visit specific websites. Only later do victims realize that these claims were a confidence trick and that they have been manipulated.

These tactics are popular because they work. It is important for you to verify who people are before you give them any personal or business information.

Be aware. Protect your business and employees by advising employees to do the following:

- Be suspicious of any phone calls, visits or email messages from individuals asking about employees, their families and sensitive business matters. This should be reinforced as part of an ongoing security awareness program.
- Ask anyone making unusual inquiries to verify their identity with official documentation. When in doubt, ask a supervisor or a colleague for help.
- Follow email, social networking, browsing and other safe practices (as described throughout this guide), and always protect personal information online.
- Always report any suspicious activity, including social engineering attempts, to a supervisor. This is especially important if you think that your business has been compromised.

Web Security

- If your business may have lost or revealed sensitive information as part of such an incident — or if there is a suspicious pattern of inquiries — determine what assets may be at risk and take action to further safeguard them. For example, if there is reason to believe your business banking information may have been obtained, contact your bank immediately and ask for assistance in protecting your accounts.
- Consider reporting the incident to the police.
- Contact the Canadian Anti-Fraud Centre and ask for advice or file a report.

A big part of cyber security involves being alert to things that seem to be "out of the ordinary." Your employees should always feel that they can report security questions, concerns or observations to someone in authority (technical or business) who will listen, document what occurred and take appropriate action.

4.5 Software Security

Your business's cyber security is only as good as the software you use. In fact, if you make all of your software secure, a large number of security threats will be reduced or resolved.

Software can include the following:

- Desktop applications (apps).
- Mobile device apps.
- Web server and related software.
- Operating Systems (OS) and more.

Software can have issues (usually known as "bugs") that can make it insecure. These bugs can be exploited by attackers and allow them to access your information. Sometimes, software will also carry malicious software — commonly referred to as *malware*.

Apply security updates to your software as soon as they are available from the developer.

Tips to maintain software security:

- Only use legitimate software that has been tested and used by others. This can include software from known vendors or independent software developers who may even provide the software for free.
- Do not use unauthorized versions of software illegally downloaded through online file-sharing systems as it is often infected with malware. Illegally copied software is not supported by developers, which means that your business cannot expect any sort of technical support if you experience problems.
- Limit access to shared applications only to those who genuinely need it. Sometimes this is done in the software itself and sometimes through the operating system.

Web Security

- Minimize the number of employees with administrative privileges to software, especially important applications and security safeguards. This will make your business less vulnerable to internal error or external attack. Many attackers target user accounts with administrative privileges because it gives them a high level of control over software and systems.
- Most importantly, apply security updates (patches) to your software as soon as they are available. Some software update notices are automated, but for others you will need to check the vendor's website regularly.

4.6 Safe Hosting and Business Web Security

If your business's website is not properly secured it could be easily compromised, which could lead to vandalism, disruption of service, or the theft of business or client data. All of these can have severe consequences.

Websites vary from business to business, but there are some basic tips to follow:

1. If hosting your website(s) internally on servers belonging to your business:
   - Restrict access to authorized employees only.
   - Apply all available and relevant patches to the Web server operating systems, and any other software that is running, to help resolve any known issues.
   - Implement regular backups of your business systems to a server at a separate location.
   - Turn on server logging and have whoever is in charge of the server(s) review those logs regularly and keep an eye out for suspicious activity.
2. 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.
3. Do not post any personal emails on your business website as spammers and others will use them (e.g., for phishing). Use generic business accounts like sales@yourbusiness.com or support@yourbusiness.com.
4. Be prepared in case your business website is compromised. You may need to reduce service, switch to a backup server or service provider, or even take your site offline temporarily. Consider all of this *before* a security incident takes place so everyone in the business knows what needs to be done.

Web Security

4.7 Malware

Malicious software (*malware*) is any software created and distributed to cause harm or steal information. Malware is designed to hide within the operating system and avoid security safeguards. It may be impossible for you to detect or remove without specialized tools or expertise. Malware exists for all of the information processing systems that may be in use in your business, including desktop computers, laptops, smartphones and tablets.

The most common type of malware is the *virus*. A virus is software that can copy itself from one system to another, infecting each computer along the way. Once a virus has infected a business system it can delete or corrupt your files, steal data or even (in rare cases) damage hardware. Viruses can originate as email attachments, website downloads or on infected disks shared between users.

Many other types of malware exist but all share the same objective: to capture and steal sensitive information (e.g., passwords) and transmit this information back to its originator without the knowledge of the system user.

Use anti-malware software to scan all incoming files and block anything suspicious or that is embedded with malware.

While dealing with malware can be challenging, you can counter a lot of these threats with anti-malware software that scans incoming files (e.g., email attachments) and blocks files if they are suspicious or confirmed to include malware. The same software will scan for infections that may already exist, warn users and provide clean-up options. Some malware cannot be removed without the help of a security expert. Prevention is always best. Install your malware safeguards before you get infected.

Most anti-malware software today covers all the types of malware described in this section, but some are still referred to as “antivirus software.” Before buying or using anti-malware tools, check what types of malware it addresses and find out how often the software is updated. The more frequent the updates, the better, as new malware appears hourly.

Your business may also need a firewall to help block connection to malicious websites and to stop some forms of malware before they are downloaded or brought in with emails.

Implementing anti-malware software and a firewall is a great first step toward strengthening your business’s cyber security. Good employee habits are also essential. All employees need to be provided with security awareness training and policies that explain their responsibilities. For example, they should be warned that they are not allowed to tamper with or disable security safeguards, including anti-malware software.

Web Security

Here are some things you should tell your employees to look out for:

- Watch for warnings on websites or emails that have been flagged as potentially dangerous.
- Report (e.g., to a supervisor or technical support person) any alerts from the anti-malware software in their work computer — including alerts that indicate that the software is out of date or has identified a suspicious file.
- Never forward suspicious emails or files to others in your business.

4.8 Authentication Best Practices

Authentication is a security practice designed to verify that a user is who they claim to be, prior to granting them access to specific systems or services that your business uses.

4.8.1 Passwords

Passwords are widely used to protect access to business information and online tools, but if employees are not careful, others can use their passwords to access crucial files and information.

There are several common problems with the use of passwords in businesses:

- Employees write their passwords down and post them in places where others can copy them — or they simply share their passwords with others. In both cases, the loss of control over that password makes it impossible to guarantee that the person accessing systems is actually authorized to do so.
- Employees use weak, easy-to-guess passwords, making it possible for others to gain access to sensitive systems or information.
- They re-use the same password across multiple systems or services so that if one is compromised, all are at risk.
- They do not change their password regularly.

Have a strong password policy that identifies what rules apply to passwords used in your business. The following guidance should be included in that regard:

- Avoid common words such as “password” or “login.”
- Avoid simple sequences of numbers such as “1234.”
- Avoid easy-to-guess personal names such as a child’s first name.
- Create passwords that are at least eight characters in length — the more characters that are used, the more secure passwords will be.

- Create strong passwords by including a combination of the following:
  - Uppercase letters.
  - Lowercase letters.
  - Numbers.
  - Special characters (e.g.: !, $, #, or %).

Explain to your employees that strong passwords are important to the security of the business, and that they should do the following to protect their password:

- Keep their passwords confidential.
- Change their passwords regularly. Your business should require employees to change their login passwords every three months.
- Avoid use of the same password for multiple accounts or systems.

Alternatively, you could consider using a password manager (a program that generates and stores random passwords) that creates even stronger passwords for employees to use.

4.8.2 Passphrases

If you need enhanced security, consider using a passphrase instead of a password. A passphrase is a whole sequence of words. For example, instead of the password "Mypassw0rd," the passphrase "!mgladMypassw0rdisgr8!" would be much harder to guess.

A passphrase that is an acronym reduces the number of keys involved. For example, "I am so glad I went on vacation in January as I love the sun!" would become "IASGIWOVIJAILTS!" Even this kind of acronym is more secure than a regular password as it is longer, more complex and unpredictable, making it very hard to guess — even with the software tools that cyber criminals use.

There are a number of free tools online that you can use to demonstrate the relative strength of passwords. While different tools may yield slightly different results, trying several will give a good indication of the strength of your chosen password.

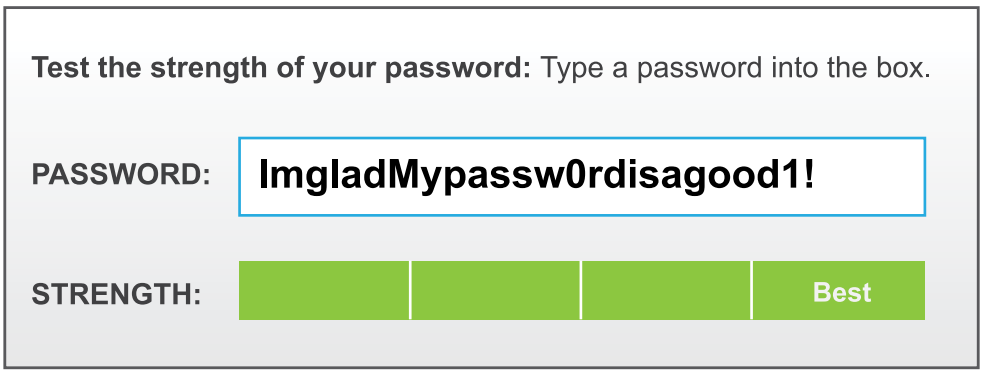


Figure 3: Passphrase Strength Example

4.8.3 Two-Factor Authentication

Two-factor authentication (2FA) is a security practice that adds another means of identification, which can make a business system much more secure.

The first factor is something the person knows (e.g., a password) and the second factor is something additional to be used in confirming the person's identity. The second factor can be something the user always has (e.g., their fingerprint, which is now used at many border crossings) or something they temporarily have, such as a one-time password (OTP). Unlike a regular password, an OTP cannot be guessed and as the name suggests it cannot be re-used either.

An OTP is generated by the user with either a secure app (e.g., on their smartphone) or a dedicated hardware device (often called a token). Either is portable and can be used as needed. In combination with a regular user name and password, an OTP greatly enhances authentication security.

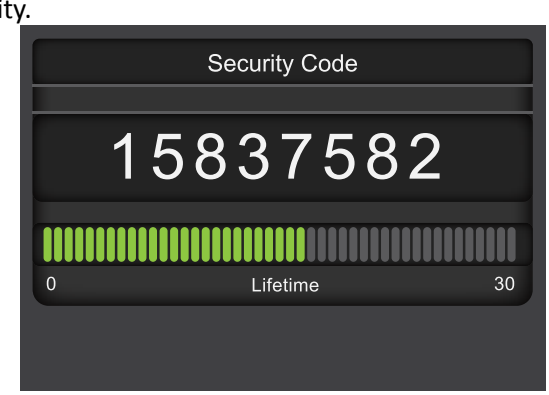


Figure 4: An Example of an OTP Showing that it Will Expire in 17 Seconds

It is strongly recommended that you implement two-factor authentication in your business especially with respect to the protection of critical systems and information. You can often start implementing two-factor authentication with simple services, such as webmail and some banking, to get a sense of how it works and then expand its use as your time and budget allow.

Point-of-Sale (POS) Security

Quick tips from this section:

- Make sure your POS system is behind a firewall.
- Set up strong encryption for all transmitted data.
- Do not use the default username and password provided by the manufacturer.
- Limit access to client data to those employees who absolutely need it.
- Ensure that all anti-malware software is up to date, as frequent security updates occur to fight new types of malware.
- If you have any concerns with the security of your POS system, contact the POS service provider.

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 to access your computer networks, and it is extremely important to protect them. Cyber criminals can hack into POS systems to steal payment card numbers and the associated personal identification number (PIN), which they can then use to access your customers' accounts.

There are 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. A firewall is a security control, which is used to restrict incoming and outgoing network traffic. Your Internet Service Provider (ISP) may include a firewall with the router or other hardware or software that they provide you, but it is important to check. If they don't provide one, you will need to purchase one.
- Set up strong encryption for the transmission of all data (e.g., cardholder data) between your POS system and the POS service provider. The service provider should implement 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.
- Do not use the default user name and password for your POS system (which will have been shipped with it). Cyber criminals will use those credentials to gain access to your system. Instead, set up a new user name and password that is unique to your business.
- Always limit access to client data only to those employees who have a need to access it and are authorized to do so.
- Keep anti-malware software up to date.

Email Security

Quick tips from this section:

- Implement a spam filter — doing so will help you get rid of most potentially harmful emails sent by cyber criminals.
- You should not 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.
- Keep your employees' emails and information confidential, as information on any member of your business can be used to hurt employees or your business.
- Enable HTTPS, which encrypts data and essentially makes it impossible for cyber criminals to access the information in your browser, for Web-based email.
- Set strict password standards for all email accounts (business or personal) being used at work.
- When possible, use generic emails (such as info@companyname.com) for email addresses that are posted in public places (such as on your website or on social media).
- Do not forward potentially harmful emails to other employees.

A number of security concerns have developed with the universal adoption of email including spam, phishing and the non-secure exchange of confidential information. These are all things that could have a negative effect on your business.

6.1 Spam

Spam is email that has been sent without the permission or request of the person it has been sent to. Spam represents approximately 69% of all email sent over the Internet.[1] Not only can spam contain links that if clicked on could harm your business, but spam can slow down your networks, servers and computers, increasing costs and reducing productivity.

Spam is used widely to:

- Sell you a product or service (much like telemarketing, but by email) and make you visit an unsafe website, leading to the download of malware onto your computer.
- Convince you to disclose confidential personal or business information (such as passwords).

[1] http://www.symantec.com/security_response/publications/threatreport.jsp

Email Security

How to identify potential spam

Here are some ways you can identify potential spam:

- If you don't recognize the sender, treat it with caution.
- Look for misspelled words in the body of the email. This is a trick fraudsters use to bypass spam filters (see the explanation to follow).
- Look for unusual phrasing in the message, which may suggest that the author is not legitimate.

Always be suspicious of emails that contain the following:

- Offers that sound too good to be true.
- Requests that you click on a link in the message.
- Requests for your personal information.

Spam is annoying and potentially harmful to your business. But there are some ways you can deal with it:

- Implement a spam filter that will block most spam and only allow legitimate and acceptable emails to get to you. If your business is using email hosted by another company, ask them about what spam filtering services they offer. If it is not working well, ask for a better spam filter or change email service providers.
- Keep your employee email list confidential. If you need to share an email address with someone outside of your business, use a generic email, like customerhelp@yourbusiness.ca.
- Develop a basic set of email guidelines for your employees and make sure all employees read and apply them. These should include the following:
  - Never click on the links that are included in spam — even if they are offering to remove you from their distribution list. This is a common trick they use to get people to visit dangerous websites.
  - Never open attachments in spam or suspected spam messages.
  - Do not write to the spammer for any reason, even if it is to complain. Doing so will only confirm that your email address is valid and will actually result in more spam.
  - Delete spam if you are certain it is not legitimate. If you are uncertain about what to do, ask a supervisor or technical support person for help. Generally, if your business does not have a technical support person available, it is best to contact the email service provider. In the worst cases, if you suspect there is a significant risk to your business, you should contact the authorities as listed in Appendix C.

Email Security

6.2 Phishing

Phishing is a specific kind of spam that targets you by simulating a legitimate message from a bank, government department or some other organization, in an attempt to get you to give up confidential information that can be used for criminal purposes.

Often these messages are written to seem helpful or will offer "good news" (Figure 5) so that you will be more likely to trust the sender and follow instructions in the email. In other cases they try to incite fear and get you to send a reactionary reply (e.g., "...your bank account is being closed. Click here to take urgent action.")

Because these messages often appear to be from real organizations — possibly using real logos and familiar colours, layout and fonts — it can be hard for you to recognize it as illegitimate. In almost every case, the message will include a website URL (link) that they want you to click and a *request or demand for confidential information.*

What to do with potentially criminal email

If you receive offensive, abusive or potentially criminal email (whether or not it seems to be spam) — or if you think you are being asked for confidential information by criminals — you should save the message (do **not** email it to others) and contact your supervisor or IT support personnel. You may be asked to provide a copy of the message to help the authorities with any subsequent investigation, which is why you should not delete it unless told to do so. See Appendix C for more information on who to contact.

Figure 5 [1]

[1] http://www.cra-arc.gc.ca/ntcs/nln-rfnd-eng.html

Email Security

Strategies for dealing with phishing should align with your business's approach to spam and should begin with spam filtering. All of your employees should be alerted to this issue and understand that any apparent phishing emails containing personal information on employees might need to be reported to the Canadian Anti-Fraud Centre.

Some additional tips to give employees on phishing:

- Do not answer suspicious emails or provide any confidential information requested in emails even if they appear legitimate. If uncertain, speak to a supervisor.
- Do not click on any links in suspicious emails.
- Do not forward the email to others. If you need to show it to a supervisor, ask them to come and see it on your screen or print it out.
- If a suspicious email appears to be from a recognized organization or client, contact the legitimate client or organization through another means of communication (e.g., by phone) and ask if they sent such an email.

6.3 Sending Email Securely

Phishing and spam are two issues associated with your *incoming* mail, but what about the security of your *outgoing* email?

As email often contains sensitive and confidential information, and is relatively easy to compromise, you need to implement appropriate security measures to:

- Make sure that only authorized employees can send emails from your business.
- Maintain the confidentiality of your messages or email attachments until delivered to the intended recipient.
- Archive your sent email for future reference (e.g., in case of an investigation or for financial or legal reasons).

Once criminals have access to a legitimate account in your business, they can use it to get the contact information associated with that account, send out spam, launch phishing attacks and more.

Enable the security protocol HTTPS for all communication between business computers and webmail servers. This will help to maintain email confidentiality.

Your business should choose a single email service for your business to help you simplify security measures. Security should be one of the key criteria in selecting an email service. If you use a webmail service, enable the security protocol HTTPS (Figure 6) for all communication between business computers and the webmail servers. HTTPS will encrypt all emails you send and receive, which will help to maintain message confidentiality.

Email Security

Develop email guidelines for employees that include the following:

- Always follow the company's password standard, including the use of a strong password for email whether the account is inside the business or hosted as webmail. This is important with webmail services, as they are more accessible for cyber criminals who will use compromised accounts for other criminal activities (such as emailing spam).
- Use the recommended security and privacy settings in the Web browser or email client software unless the person responsible for cyber security in the company tells you to change them. The security features built into those applications are there to protect the business. (In your business, it is possible that your employees set up their own email software. If that's the case, it is best that they follow the security recommendations of the browser or email client developer).
- Before sending emails or attachments that contain sensitive information, always ask yourself: "Could the unauthorized disclosure of this information cause serious harm to me or my business?" If the answer is "Yes," then use another more secure method.
- If there is a need for you to send potentially sensitive information outside of the business, ask the recipient to verify that they received it. Also, encrypt attachments (e.g., Word documents) before sending them over the Internet. See Figure 7.

Figure 6:
HTTPS is enabled

Write and follow an email retention standard appropriate for your business and any provincial or federal legislation. For example, if your business is required to keep client records for seven years — and you communicate with clients by email — then you need to maintain email archives for at least seven years. This can be done by backing up your email to an internal storage system or by arranging scheduled backups with your email service provider. If you are not sure how long you need to keep emails, check with your lawyer, accountant or another responsible party to confirm any requirements. Once email archiving is set up you will be ready if called upon to provide older emails.

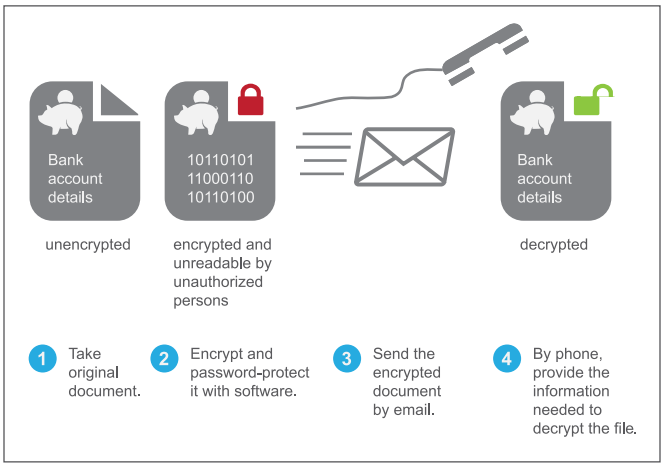


Figure 7:
Encrypting an Attachment

Data Security

Quick tips from this section:

- 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.
- Download or purchase automatic backup software to ensure timed backups of your system(s).
- Store your physical backups (e.g., external hard drive) offsite in a safe place.
- Have emergency system boot DVDs or USB sticks prepared in case of a system crash.
- Properly label any sensitive information you have to ensure secure handling.
- 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.

7.1 Backup and Recovery Options

A backup plan is essential for your business. Without one, your business will risk losing critical information (such as client records) and services (such as payment processing). Such losses can hurt your operations, damage your reputation, result in legal action or even cause the failure of your business.

Backups are used to restore lost or damaged files. Backing up data will help ensure that your business is able to recover quickly and completely when a system crash, data corruption or other setback occurs.

There are several options you can use for backup and recovery including the following:

1. **Portable or desktop USB hard drive:** This is a good place to start if your business only has a few computers. You can provide one drive for each computer or share one for up to three systems. Backup software will allow you to automate this process and track changes to your data between backups. The same software will allow you to restore anything from a single file to the entire system.
2. **Server:** If your business has a Local Area Network (LAN), data should be stored on your server and backed up from there. Server backups can be completely automated and run as often as needed.
3. **Online:** Another option involves backing up your data to the Internet. Backup and restoration service providers will maintain copies of your business data. Online backups might not be suitable for:

    - Your highly valuable or sensitive data.
    - Storage of private data on behalf of Canadian clients or patients — especially since many online backup service providers operate outside of Canada.
    - Restoring your data quickly as local backups are typically faster.
    - Guaranteed on-demand data restoration, since the Internet can go down.
    - Continuous or very frequent backups, which can overwhelm your Internet connection and prevent other work.

Data Security

Best practices when backing up or restoring information:

- Have a plan and begin your backups as soon as possible. Start by backing up all files and folders that may be of value. This is often referred to as a "full" backup and it sets a foundation for future backups. After this, you will only need to backup new or modified files and folders.
- Back up your data regularly, whether it is daily, hourly or as appropriate for your business.
- Choose a backup application with automatic and continuous backup to make sure that your backups are completed.
- Keep copies of your backups in a secure location off-site. The idea is to protect the backups from theft or a disaster (such as fire). If an off-site location such as a bank safety deposit box is impractical, consider getting a small fire-resistant safe. Ensure off-site backups are kept up to date.
- Always include system and software settings as part of your backups.
- Have emergency boot discs or USB sticks ready in case of a system crash and keep at least one copy off-site with other important backups.
- Test your backups periodically by recovering an important file, folder or even a whole drive. When there is time, at least once a year, also do a complete system restoration to a "test" computer (e.g., not a computer that is in use by your business) to make certain that your business can use the backups on hand to perform a complete system recovery in the event of a disaster.

Things to think about when developing your backup plan:

- What do you need to back up? Build a list of your critical files and where they are located and you will know what you need to back up.
- How often do you need to back up? Some data may change infrequently while other files change all the time. If the information is important, back it up as often as you need, which may be once a day, hourly or even more frequently.
- How long should you keep backups? You may only need to keep the most recent backups, or you may have legal or contractual obligations to keep some data for specific periods — possibly years. Check with your lawyer, accountant or another responsible party to confirm the requirements.

Data Security

7.2 Cloud Security

Cloud computing is using resources and programs that are available on the Web, outside of your business. You may be familiar with cloud services like data storage, but cloud computing also includes billing and payment services, document and account management, and marketing and productivity tools.

There are many reasons for a small- or medium-sized business to consider using cloud computing. Cloud services offer powerful software, similar to what is used in much larger companies, at competitive prices. What's more, some services allow for customization to fit your business's needs, and can offer the flexibility to access cloud services from nearly any device that connects to the Web. Finally, a good cloud services provider will support their products to improve their security and stability.

As attractive as cloud computing is, cloud services mean that you will be placing data in the hands of someone outside of your business, so you need to be able to trust how they will handle that information. Your business needs to consider several security issues in deciding whether a cloud service is right for you.

1. Read reviews and get recommendations on potential cloud service providers. Research the security capabilities of potential cloud-computing service providers, including the following:
   - Anti-malware protection.
   - Software patching and maintenance.
   - Strong encryption during the movement of data and while information is stored.
   - Redundant power in case of a power failure.
2. Beyond security, ask about a cloud service provider's reliability, service levels and past performance. For example, you can ask how they back up their data and what happens if the service goes down.
3. Manage access to your cloud services. You should decide who in your business can access a service, and what account privileges they will have. Decide whether employees can access business data on personal devices and the procedure to follow if a device is lost or stolen. If an employee leaves, be sure to remove their access to your services.
4. Exercise your due diligence. Talk to your legal counsel to understand what liabilities you may face if client information were lost or stolen while hosted in the cloud, and look closely at agreements with cloud service providers on who owns products and bears responsibility for the data.
5. Understand any federal or provincial legal requirements related to storing different kinds of information. Information uploaded from Canada may be stored on a server in another country. Depending on your line of business, government regulations may stipulate how your data is handled, including where it is stored, for how long and the level of security required. This is especially true with respect to medical or financial records that your business may hold.

Data Security

Using a Secure Cloud-Based File-Sharing Service

One aspect of cloud computing that your business may find useful is file-sharing and synchronization services. These allow you to upload files to the cloud for clients, consultants or other personnel to view, download and modify. If changes are made by any of the users, files are synchronized so that everyone has access to the most current version.

Your business can limit associated security risks by doing the following:

- Considering which types of information can be safely shared this way.
- Choosing a service that requires users to login, ideally with two-factor authentication, so only people you authorize can access the shared files.
- Limiting the number of people with access to those who need it.
- Using a service that can send you notifications when a file is received or changed.
- Encrypting sensitive information before you upload or share it.

7.3 Classifying and Labelling Sensitive Information

Classifying and labelling sensitive information is critical to its secure handling in your business. Many classification systems can be employed to help determine how sensitive information is and then to label it (e.g., as documents, files, records, etc.).

The key is to have a system in place that all of your employees understand and follow. Your business will need to develop a method for classifying information and guidelines for labelling and handling that information.

How to determine which information is sensitive:

1. Identify your information and where it is located (e.g., on a server, in the cloud, etc.).
2. Ask yourself what harm would result from the loss or theft of each group of information your business holds. Rate the loss from 1–5 where 1 is “insignificant” and 5 is “catastrophic.” Sort the results.
3. Information that is rated higher is more “sensitive” and should be labelled and handled with proper care for its security (e.g., control of access, backup, etc.).

A simple classification model is easier to remember and follow. For example:

1. **Public** information is available to everyone and anyone, inside or outside of your business, and requires no protection or special marking or handling. News posted to your business’s website is an example of public information.

Data Security

2. **Restricted** information needs to be protected in some manner and is usually limited to a select group of people including employees and certain clients, service providers or others. This information would be controlled through various security safeguards you have put in place and should be labelled "Restricted." An example of restricted information is payroll information.
3. **Confidential** information is limited to access by select individuals in your business. Its loss or exposure could damage your business. Confidential information must be labelled, carefully handled and should not be allowed to leave business premises or systems. An example of confidential information is intellectual property owned by the business or sensitive client data.

You should document and explain to employees or affiliates (e.g., for banking) the rules on how information should be labelled, handled or shared, including the following:

- Always checking the classification of information to determine how it should be handled.
- When using or sharing classified information, limiting access to those who are authorized.

7.4 Handling Sensitive Information

Some of your business information will be particularly sensitive (e.g., financial or customer records), meaning that the unauthorized access to, loss, misuse or modification of that information could cause serious harm to your business or clients.

Tips for handling sensitive information:

- Lock up and restrict access to sensitive information when it is not being used. With digital documents this will involve a combination of electronic and physical safeguards to limit access only to authorized employees or clients. For paper documents it may involve locked filing cabinets or a safe.
- Always label sensitive information and train employees to follow guidance on the handling of labelled information. If information is not labelled, employees should ask for assistance or clarification to make sure they are handling it correctly. Digital information can be grouped by sensitivity on a common server, in a specific database or individually labelled.
- If you have to destroy any sensitive information, the electronic destruction methods must also be thorough. Usually if you "delete" a file on your computer, the file is not actually removed until the space is overwritten by something else. Commercial "secure erase" or deletion tools can completely destroy your sensitive information, much like putting a paper document through a shredder.
- When you dispose of storage media, it is best to destroy it physically. For example, CDs and DVDs can be put through some paper shredders.
- When destroying paper records, a high-quality shredder that crosscuts the paper into small pieces should be used, or consider paying a professional document and media destruction company.

Remote Access Security

Quick tips from this section:

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

Providing remote access to your business network and information allows you and your employees to work from home or while on the road, saving time and money, and increasing productivity. But allowing remote access can expose your business to cyber threats. Many of these threats can be addressed through good security habits on the part of employees along with strong technical safeguards you can put in place.

8.1 Remote Computing Security Basics

If employees are provided with remote access to your business's computers, it will normally be over the Internet and should involve the use of a secure *Virtual Private Network* (VPN).

A VPN is an extension of your business's internal network (or from one computer to another) over the Internet. The Internet is not considered secure for the exchange of confidential information on its own, so all traffic in a VPN is encrypted, rendering it unusable to anyone except the legitimate sender and receiver. A VPN is a proven solution that is relatively simple for you to set up with commercial or free software or as a service. Some hardware, such as a router and firewall, is also required.

Once in place, a VPN can allow your users to access and share business files or applications from their remote location, and to communicate with fellow employees using email, as if they were in the office.

A VPN should always be used with other security safeguards (as described in this guide) including up-to-date anti-malware software and two-factor authentication.

Below are some basic steps you can take to protect your business with respect to remote computing:

- Limit remote access to authorized employees with a clear business need. Access should only extend to the applications, information and services that are required for work to be performed.
- All employees authorized to have remote access privileges should be required to sign a simple Remote Access Agreement to indicate that they understand the associated rules and responsibilities.

Remote Access Security

- You should adjust remote access privileges as responsibilities change. For example, an employee moving from Accounting to Sales may no longer need access to certain accounting resources so their access should be changed. Remember to revoke all remote access privileges when an individual leaves your business.
- When possible, provide employees with business computers, configured with appropriate application software, remote access tools and security safeguards, instead of using their home computers.
- Record serial numbers for all personal computing devices used for remote access or work outside of the office — including laptops, smartphones and tablets — to help track their configurations (including security software) and to help with recovery if they are lost or stolen. This information will also help with police reports and insurance in the case of theft or loss.
- Label all your business computers that are used outside of the office with your business name, contact information and an asset number.

8.2 Working From Home

Logging in to work from home is convenient for you and your employees. But working from home on a personal computer introduces some additional risks that need to be addressed:

- As part of the wireless system, a small device called a cable or Digital Subscriber Line (DSL) modem connects home networks and computers to the Internet. Usually, a router is also required for communications inside the home. Your employees should connect the computer directly to the router using a standard Ethernet cable. Similarly, the router should be connected, via an Ethernet cable, to the modem. If these steps are taken, there is no wireless communication that can be listened to by outside parties.
- When using Wi-Fi, you must secure it so that potential attackers cannot monitor the home network and steal your business's sensitive information. To guarantee a secure connection, all employees should be required to do the following:
  - Change the default Wi-Fi network name and the router access password on the network router. The name is called the Service Set Identifier (SSID) and changes can usually be made quite easily online, following the manufacturer's instructions for use.
  - Turn on network encryption to make sure that any intercepted communications cannot be used by cyber criminals against employees or your business.
  - The home work environment is only as secure as the workspace. Employees should be advised to limit access to the computer they will use for work. For example, children should have a separate computer for their own use to prevent accidental compromise of the computer used for business access.

Remote Access Security

8.3 Working While Travelling

Your business's portable computing 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.

Here are some tips for you and your employees while on the road:

- Avoid unknown, unfamiliar and 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.
- Don't leave your laptop or related materials unattended in a public workspace, even for a moment. Theft of laptops, smartphones and tablets is common and on the rise. If possible, secure laptops with a cable lock — even when attended and in sight. Lose a business laptop or other electronic device and you lose all the information.
- Make sure that you guard confidential information on your screen from curious onlookers. If you're on a flight, anyone with line of sight to the laptop can see what is on the screen. Wait to review any sensitive information in a more private and secure location. If this is not possible, dim the screen and change the laptop's position to limit who can see it.

Mobile Device Security

Quick tips from this section:

- Ensure that all of your mobile business devices (phones, tablets) have system access passwords and are locked when not in use.
- Properly safeguard data on mobile devices. Most mobile devices have security features and many smartphones and tablets can even run anti-malware software.
- Encrypt all of your sensitive data on portable storage devices.

Your business likely uses mobile devices and portable data storage (such as USB sticks) in your everyday operations. They increase productivity, make communication easier and allow you to easily carry important data.

Using mobile devices to send and receive your business's information can expose your business to the risk of sensitive information being viewed or used by people you have not authorized to do so. Allowing employees to use their business-owned mobile device for personal use, such as the installation of non-business apps, can sometimes expose your business to the loss of sensitive information, malware and other threats.

To address mobile device security in your business, it is important for you to

1. Examine the pros and cons of mobile device use in your business.
2. Determine which types of devices you will allow in the business.
3. Decide whether personally owned mobile devices can be used by employees for business purposes.
4. Develop standalone rules of use or integrate rules into your business's cyber security policy.
5. Develop a plan for the management of your mobile devices (which may include a need to access and control them remotely or to block certain functions) and buy tools to support that plan. You can begin by speaking to your mobile service provider and visiting the website of the phone or tablet manufacturer for advice.
6. Log the serial numbers of all mobile devices used in your business in case of loss or theft.

Mobile Device Security

9.1 Tablets and Smartphones

Tablets and smartphones offer incredible functionality, including the ability to create, store, send and modify data with ease. But these features can lead to accidental misuse by employees or manipulation by cyber criminals if the device is hacked or stolen.

Because these devices are small and valuable, they are common targets for theft. Whether compromised through malware, misuse, loss or theft, the impact on your business may be significant, especially if the device contains sensitive information or communications tools for connection to your business network.

Tips to help address the threats to your mobile devices:

- Treat smartphones and tablets with the same security precautions and care as desktop computers and laptops, as all of them can be compromised or stolen.
- Set up a system access password and ensure that the smartphone or tablet is always locked when not in use. Your sensitive personal or business information contained in the device will be much harder to access if the device is lost or stolen.
- Properly safeguard sensitive information on these devices, including any sensitive emails transmitted or received while travelling.
- Back up your device contents on a regular basis.
- Install and run appropriate security apps, which can include encryption, locators for a lost device and anti-malware.
- Advise employees to promptly report the loss of a business tablet or smartphone as soon as it is noticed so that efforts can be made to alert the police, recover the device or (if the appropriate software has been set up) remotely wipe device contents.

9.2 Portable Data Storage

Portable data storage can hold massive amounts of information in a very small device. Your business may even be able to store all of its electronic files on a portable storage device.

Older storage media such as CD or DVD discs are being replaced by portable hard drives and USB flash memory sticks (sometimes called thumb drives). Your business may already use one or more of these methods to store important information.

Although convenient and low cost, the use of portable data storage devices exposes your business to cyber security threats including the following:

- Infection by malware (a problem most common with USB flash drives).
- The loss of your device and all of the information on it. This problem is widespread and again most often involves USB drives, but also CDs and DVDs.
- Information on the device can be easily copied by potential criminals (as most such devices do not include any security safeguards).

Mobile Device Security

To reduce these threats, here are a few steps you can take:

- Identify the rules for use of such devices and the handling of information in your business policies (as explained in other sections of this guide); for example, make it clear what information can be stored on mobile devices, and what specific safeguards and protections need to be in place for particular kinds of information — such as encryption of client information.
- Use the safeguards available for your device. Most mobile peripherals have security features and even many smartphones and tablets can run anti-malware software.
- Label all of your portable storage devices with your business name and a contact number in case it is lost.
- Encrypt sensitive files on portable storage so that they cannot be copied or used by someone in case of loss, theft or illicit use. It may be more effective for you to encrypt the entire storage device (e.g., USB flash drive) so that all of the information placed on it is protected.
- Train your employees in the secure handling of portable storage devices to help limit theft or loss and, as with other mobile devices, advise employees to report loss of any device promptly.

Physical Security

Quick tips from this section:

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

All of your business's cyber security safeguards could be of limited effect if you do not use appropriate physical security. If a disgruntled employee or a visitor gained access to one of your computers, they could quickly and easily download sensitive data onto a memory stick. Cyber security safeguards like authentication and encryption need to be complemented by other security measures, like locks on doors and sign-in procedures for visitors.

Physical security is a topic on its own. This section provides some key tips for you and your employees:

- Only allow employees access to areas of the business that they have a legitimate need to be in. For example, sales people usually don't need to access and modify servers. Lock up the servers and only provide access to those who need it.
- Have employees follow best practices for their workstations, known as the "clean desktop" principle. Employees should put away sensitive items when not at their work area. These can include the following:
  - Documents that contain sensitive or confidential information about your business.
  - Personal information, especially if it pertains to clients.
  - Portable electronic media including CDs, USB memory sticks or other items that can be easily removed.
  - Always have employees lock their business computer when they leave their work area. They don't need to shut down the computer to do this — most operating systems allow users to enter a combination of keys to disable access until they re-enter their password.

Physical Security

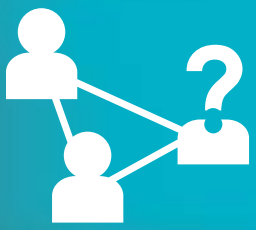
10.1 Employee Security

Employee security includes processes and practices to establish the suitability and trustworthiness of employees in order to protect the business prior to hiring, as well as ongoing vigilance around employee practices.

Some specific recommendations for you with respect to employee security include the following:

- Publish and enforce an employee security policy that defines what rules apply to employees and what discipline (including termination) is applicable in the event of a security incident where an employee is at fault.
- Always perform background checks for all new employees. References alone are not always sufficient given the potential for fraud through social engineering.
- Be clear about how non-competition, non-disclosure, intellectual property rules and contractual obligations apply in the context of your business's cyber security. For example, you should tell new employees that emails to competitors are not allowed without prior approval.
- Clearly communicate security responsibilities to new hires and contractors as part of their orientation, and have them formally acknowledge that they have read and understood the material including all cyber security-related policies.
- Clearly state and enforce the consequences of security lapses especially where employees may have ignored or broken rules or caused harm to your business.

Finally, the employee termination process is relevant to your business's security. There have been many cases of former employees accessing internal networks and stealing data or planting malware. When an employee or contractor is terminated or indicates that they are leaving, access to your business's computers and information must be terminated, and business property such as laptops, keys and access badges returned — as soon as possible after termination.



Getting Help

11.1 When to Ask for Help

If you run a small or medium business, you might not have the expertise on hand to manage all aspects of cyber security. You may need some assistance in choosing and implementing some security solutions.

If you don't think you can handle your security needs on your own, we recommend your business seek outside help from individuals or companies that specialize in cyber security. Look for companies with good reputations, knowledge and expertise in the areas where you need help.

Some cyber security solutions, such as online backup of all your data, might be impractical to manage on your own. Cyber security companies can help provide this kind of long-term service, including customer support, more effectively than you could in-house.

Finally, in cases of serious cyber attacks, it may be necessary to contact the appropriate authorities. If your business or any of its employees are threatened or harmed through a cyber security incident, contact the police. Appendix C provides a list of other contacts you might find useful when dealing with a cyber attack.

11.2 Where to Get Security Safeguards

To find such security tools you will often need to consult with outside experts and vendors to determine what is needed and to understand the options. Some free options exist, but most cost money initially and over time.

A lot of security software is available on the Internet for free. Always check for user comments online to see what others have experienced, talk to other small business owners, and research the source, history and validity of free software before using it. Make certain that it is widely accepted as legitimate and is not a form of malware. Paying for security software usually includes vendor support, including a warranty, technical support for set-up, as well as updates. The cost can vary widely and can extend across several years as licenses for software or maintenance are renewed, often annually.

Appendices

12.1 Appendix A: Cyber Security Status Self-Assessment

These questions will help determine your business's basic status with respect to cyber security. Answering these questions before reading the guide will help you determine which sections to focus your attention on.

These questions are based on the assumption that your business (irrespective of its size)

1. Uses computers for business purposes.
2. Uses mobile computing or communications devices for business purposes.
3. Connects some or all of those devices to the Internet for business purposes.
4. May also have an internal network, used to share applications software, peripheral devices (such as printers) and information within your business.

For each question, please circle one answer. If you don't know the answer or are unable to understand the question, then select "Not sure."

Total up your score by adding together the numbers to the left of your answers. For example, if you answered "Not sure," then that answer will have a value of zero (0), or if you answered "Yes," then the value would be two (2).

Business Questions

1. Is cyber security a priority for your business?

0. Not sure
1. No
2. Yes

2. Has someone in your business been given responsibility for cyber security?

0. Not sure
1. No
2. Yes
3. If yes, is this an ongoing role, supported by management (circle if yes)?

3. Has your business completed a cyber security threat and risk analysis (of any kind)?

0. Not sure
1. No
2. Yes
3. If yes, are risks prioritized and tracked with regard to reducing them (circle if yes)?

Appendices

4. Does your business have a Cyber Security Plan?

0. Not sure
1. No
2. Yes
3. If yes, is it being followed (circle if yes)?

5. Does your business have a Cyber Security Policy?

0. Not sure
1. No
2. Yes
3. If yes, is it supported through security awareness training for employees (circle if yes)?

6. Does your business have a Disaster Recovery Plan?

0. Not sure
1. No
2. Yes
3. If yes, is it kept up to date and has it been tested (circle if yes)?

7. Does your organization provide employees with guidance on the handling and labelling of sensitive information?

0. Not sure
1. No
2. Yes
3. If yes, is this supported by policy or a standard (circle if yes)?

8. Does your organization provide employees with guidance on the secure use of mobile devices?

0. Not sure
1. No
2. Yes
3. If yes, is this supported by a guideline and any mobile device management tools (circle if yes)?

Appendices

Technical Questions

9. Is there a firewall installed between your business computers, including point-of-sale (POS) systems, and the Internet?

0. Not sure
1. No
2. Yes
3. If yes, is it regularly maintained and checked by someone with the appropriate training and experience (circle if yes)?

10. Does your business use an encryption tool (usually software) to secure sensitive information before sharing it outside of the business environment (such as with the transmission of email attachments)?

0. Not sure
1. No
2. Yes
3. If yes, do all personnel know how to use the tool and is usage monitored and enforced (circle if yes)?

11. Does your business have a spam filtering or blocking solution in place?

0. Not sure
1. No
2. Yes
3. If yes, do all personnel know how to report spam that is threatening or seems to be part of an attempt to solicit personal or sensitive business information (circle if yes)?

12. Does your business use an anti-malware solution?

0. Not sure
1. No
2. Yes
3. If yes, is it installed on all of the business's computers and is it regularly (usually hourly or daily) updated (circle if yes)?

13. Does your business follow best practices for strong passwords and password protection?

0. Not sure
1. No
2. Yes
3. If yes, are strong password rules enforced (circle if yes)?

Appendices

14. Does your business back up data and applications on a regular basis (usually daily or more frequently)?

0. Not sure
1. No
2. Yes
3. If yes, are backups tested on a regular basis and are some backups kept off site in case of disaster (circle if yes)?

15. Does your organization provide personnel with guidance on working in a secure manner when travelling or otherwise outside of the business environment?

0. Not sure
1. No
2. Yes
3. If yes, is this supported by use of a virtual private network (VPN) (circle if yes)?

You have finished the self-assessment questionnaire.

If your score was **0-to-15** then you should consider reading this whole guide, as soon as you can. Then, consult with others in the business to begin planning and implementing cyber security in your business.

If your score was **16-to-30** then it's safe to say that your business has done some work with respect to cyber security. However, you likely need to do more and should read the guide with particular focus on those areas where you scored low.

If your score was **31-to-45** then your business has made good progress in several areas of cyber security. However, new threats are constantly developing and it will be important to still consider the topics in this guide and discuss next steps (as appropriate).

Appendices

12.2 Appendix B: Glossary

Assets: Any items belonging to or held by the business, with some value (including information, in all forms and computer systems).

Attack: An attempt to gain unauthorized access to business or personal information, computer systems or networks for (normally) criminal purposes. A successful attack may result in a security *breach* or it may be generically classified as an "incident."

Authentication: A security practice implemented (usually through software controls) to confirm the identity of an individual before granting them access to business services, computers or information.

Backup: The process of copying files to a secondary storage solution, so that those copies will be available if needed for a later restoration (e.g., following a computer crash).

Breach: A security breach is a gap in security that arises through negligence or deliberate attack. It may be counter to policy or the law, and it is often exploited to foster further harmful or criminal action.

Cyber: Relating to computers, software, communications systems and services used to access and interact with the Internet.

Encryption: Converting information into a code that can only be read by authorized persons who have been provided with the necessary (and usually unique) "key" and special software so that they can reverse the process (e.g., decryption) and use the information.

Firewall: A firewall is a type of security barrier placed between network environments. It may be a dedicated device or a composite of several components and techniques. Only authorized traffic, as defined by the local security policy, is allowed to pass.

HTTPS: Hypertext Transfer Protocol Secure.

Identity Theft: Copying another person's personally identifying information (such as their name and Social Insurance Number) and then impersonating that person to perpetrate fraud or other criminal activity.

Malware: Malicious software created and distributed to cause harm. The most common instance of malware is a "virus."

Patch: An update to or repair for any form of software that is applied without replacing the entire original program. Many patches are provided by software developers to address identified security vulnerabilities.

Appendices

OS: Operating System.

OTP: One-Time Password.

Password: A secret word or combination of characters that is used for authentication of the person that holds it.

Phishing: A specific kind of spam targeting one or more specific people while pretending to be a legitimate message, with the intent of defrauding the recipient(s).

POS: Point of Sale.

Risk: Exposure to a negative outcome if a *threat* is realized.

Safeguard: A security process, physical mechanism or technical tool intended to counter specific threats. Sometimes also referred to as a control.

Server: A computer on a network that acts as a shared resource for other network-attached processors (storing and "serving" data and applications).

SMB: Small and Medium Business.

Spam: Email that has been sent without the permission or request of you or the employee it has been sent to.

Threat: Any potential event or action (deliberate or accidental) that represents a danger to the security of the business.

URL: Uniform Resource Locator.

Vulnerability: A weakness in software, hardware, physical security or human practices that can be exploited to further a security attack.

VPN: Virtual Private Network.

Wi-Fi: A local area network (LAN) that uses radio signals to transmit and receive data over distances of a few hundred feet.

Appendices

12.3 Appendix C: Canadian Cyber Security Sites and Contacts

12.3.1 Canadian Government Security Sites

1. **Get Cyber Safe** provides news, tips and guidance on cyber security for individuals and businesses in Canada
   - www.GetCyberSafe.gc.ca

2. **The Canadian Anti-Fraud Centre** for fraud prevention and reporting (including cyber crime)
   - Toll Free: 1-888-495-8501
   - Toll Free Fax: 1-888-654-9426
   - Email: info@antifraudcentre.ca
   - http://www.antifraudcentre-centreantifraude.ca/english/home.html

3. **The Canadian Radio-television and Telecommunications Commission Canada** site for reporting scams by phone
   - http://www.crtc.gc.ca/eng/INFO_SHT/G9.htm

4. **Office of the Privacy Commissioner of Canada:**
   - Securing Personal Information Self-Assessment Tool: http://www.priv.gc.ca/resource/tool-outil/security-securite/english/AssessRisks.asp?x=1
   - Getting Accountability Right with a Privacy Management Program: http://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp

5. **Canada's Anti-Spam Legislation**
   - http://fightspam.gc.ca/eic/site/030.nsf/eng/home
   - Worried it's Spam? 5 Things to Look For: http://fightspam.gc.ca/eic/site/030.nsf/eng/h_00241.html

Appendices

12.3.2 Cyber Security Member Associations in Canada

Cyber security industry associations are a good source for more in-depth information and advice on cyber security for small and medium businesses. They can also provide recommendations on available service providers in your area if you need outside help.

1. **American Society for Industrial Security** (ASIS)
    - http://www.asis-canada.org/

2. **High Technology Crime Investigation Association** (HTCIA)
    - http://www.htcia.org/

3. **Information Systems Audit and Control Association** (ISACA)
    - http://www.isaca.org/Membership/Local-Chapter-Information/Browse-by-List/Pages/North-America-Chapters.aspx

4. **Information Systems Security Certification Consortium, Inc.** (ISC2)
    - https://www.isc2.org/chapters/Default.aspx

5. **Information Systems Security Association** (ISSA)
    - https://www.issa.org/?page=ChaptersContact