PENSEZCYBERSECURITE

Protégez-vous en ligne.

Connaissez les risques.

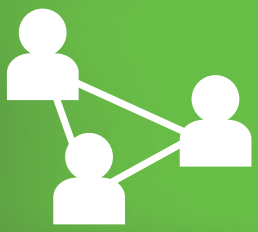
Protégez-vous.

Protégez votre entreprise.

GUIDE PENSEZ CYBERSÉCURITÉ POUR LES PETITES ET MOYENNES ENTREPRISES

Canada

Table des matières



Introduction

Si votre entreprise est comme la plupart des petites et moyennes entreprises au Canada, Internet est pour vous un outil de réussite indispensable dans l'économie numérique moderne. La navigation en ligne vous permet de joindre de nouveaux clients et de faire prospérer votre entreprise. Et, même si vous n'avez pas de site Web, de page Facebook ou de compte Twitter, vous comptez probablement sur Internet pour effectuer vos activités professionnelles quotidiennes, comme les transactions bancaires, la paie ou les commandes de fournitures.

Cependant, l'utilisation d'Internet doit se faire de façon sécuritaire. En tant que petite ou moyenne entreprise, il est facile de croire que vous n'avez pas assez d'importance pour que les cybercriminels s'intéressent à vous. En fait, les cybercriminels visent maintenant activement les petites entreprises, car ils croient que leurs ordinateurs sont vulnérables.

Le présent guide a été conçu pour aider les Canadiens qui possèdent ou gèrent une petite ou une moyenne entreprise à comprendre les risques auxquels ils sont confrontés en matière de cybersécurité; il leur fournit des conseils pratiques sur la façon de mieux protéger leur entreprise et ses employés contre la cybercriminalité.

En d'autres mots, si vous êtes propriétaire d'une entreprise, petite ou moyenne, ce guide s'adresse à vous. La cybersécurité est une responsabilité commune et, selon la façon dont votre entreprise est structurée, d'autres personnes — copropriétaires, gestionnaires ou employés — devraient vraisemblablement connaître l'information qui s'y retrouve.

Vous n'avez pas à être un expert de l'informatique ou du Web pour lire ou mettre en application les mesures qu'il propose. Certains termes propres à la cybersécurité sont utilisés, mais vous pouvez chercher ceux que vous ne connaissez pas dans le glossaire qui se trouve à la fin du guide ou en ligne à l'adresse PensezCybersecurite.gc.ca.

L'outil d'auto-évaluation de l'annexe A vous aidera à déterminer les domaines dans lesquels votre entreprise a le plus besoin d'aide. Si vous éprouvez un incident cybernétique grave, contactez la police, cherchez de l'aide professionnelle et consultez l'Annexe C du présent guide pour obtenir des ressources supplémentaires.

La cybercriminalité et les petites entreprises

- En 2012, les petites et moyennes entreprises (c.-à-d. celles comptant moins de 500 employés) employaient dix millions de Canadiens, ce qui représente presque 90% de tous les employés au Canada;[1]
- En 2012, 87 % des entreprises canadiennes utilisaient Internet et 46 % d'entre elles avaient un site Web;[2]
- Le domaine où la croissance des cyberattaques a été la plus forte en 2012 est celui des entreprises de 250 employés et moins — 31 % de toutes les attaques les visaient;[3]
- Sur une période de 12 mois, en 2012, 69 % des entreprises canadiennes sondées ont rapporté diverses formes de cyberattaques qui leur ont coûté environ 5,3 millions de dollars, soit environ 15 000$ par attaque.[4]

[1] Registre des entreprises de Statistique Canada, décembre 2011, sur l'emploi, la rémunération et les heures de travail de Statistique Canada, avril 2012.

[2] http://www.statcan.gc.ca/daily-quotidien/130612/dq130612a-fra.htm

[3] Rapport Symantec sur les menaces de sécurité Internet pour 2013. http://www.symantec.com/security_response/publications/threatreport.jsp (en anglais seulement)

[4] Rapport d'une étude de l'International Cyber Security Protection Alliance : 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 (en anglais seulement)

Fondements de la cybersécurité

La cybersécurité vise la protection de vos renseignements, souvent le bien, le plus essentiel et le plus précieux qu'une entreprise puisse posséder. La cybersécurité s'appuie sur trois objectifs fondamentaux :

- *La confidentialité* : tous les renseignements importants que vous détenez, comme les dossiers des employés, des clients ou les dossiers financiers, devraient être confidentiels. Ces renseignements devraient être accessibles seulement aux personnes (ou aux systèmes) qui ont obtenu votre permission;
- *L'intégrité* : vous devez veiller à maintenir l'intégrité de ces renseignements et des autres biens (comme les logiciels) afin que chaque élément demeure complet, intact et non corrompu;
- *L'accessibilité* : vous devez veiller à ce que les systèmes (comme les réseaux), les services et les renseignements soient accessibles, au besoin, par l'entreprise et ses clients.

L'atteinte et le maintien de ces objectifs sont un processus continu. Pour que la cybersécurité soit efficace, il faut :

1. Déterminer les biens que vous devez sécuriser (essentiellement, tout ce qui a de la valeur et qui est géré ou protégé par votre entreprise);
2. Découvrir les *menaces et les risques* qui pourraient toucher ces biens ou l'entreprise dans son ensemble;
3. Déterminer les *mesures de protection* que vous devriez mettre en place pour lutter contre les menaces et sécuriser les biens;
4. Surveiller vos mesures de protection et vos biens pour prévenir ou gérer les atteintes à la sécurité;
5. Régler les problèmes liés à la cybersécurité dès qu'ils surviennent (p. ex. une tentative pour pénétrer dans les systèmes de l'entreprise);
6. Mettre à jour les mesures de protection et les adapter au besoin (en cas de changements relatifs aux biens, aux menaces et aux risques).

Fondements de la cybersécurité

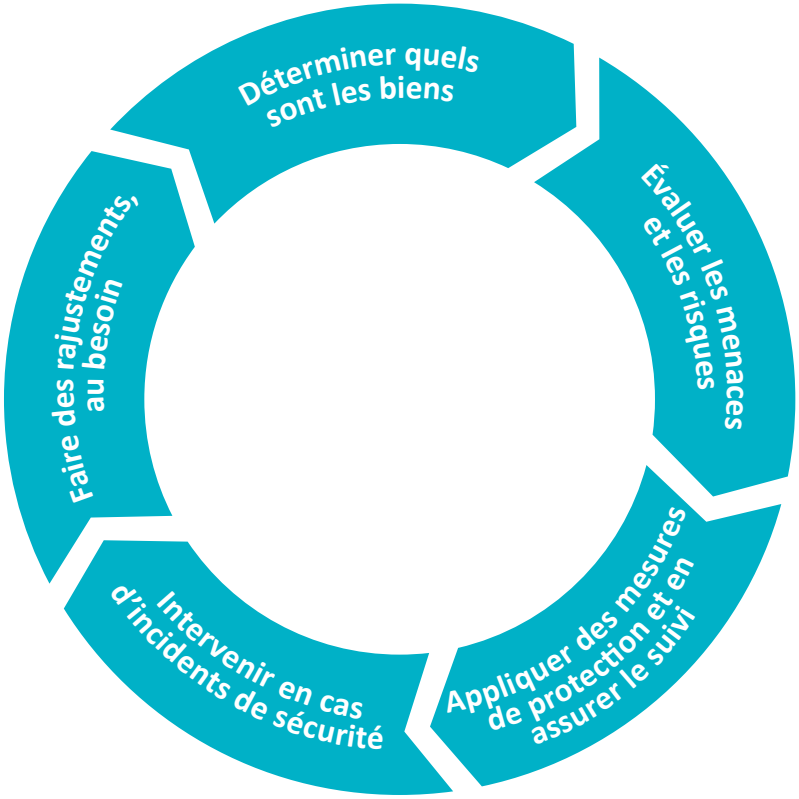


Figure : 1

Le terme *menace* signifie tout danger potentiel pour votre entreprise, ses biens ou ses employés. Les menaces peuvent venir d'une cause naturelle, comme un incendie ou une inondation. Elles peuvent aussi être d'origine humaine. En fait, les menaces d'origine humaine deviennent plus fréquentes et exigent une grande attention de votre part.

L'enjeu le plus important pour votre entreprise consiste à définir quels sont les biens, les menaces et les risques potentiels qui s'ensuivent, et à les classer par ordre de priorité. Ensuite, vous devez prendre les *mesures de protection* appropriées. Les mesures de protection sont tout ce que vous pouvez faire pour contrer les menaces et réduire le risque. Il peut s'agir de n'importe quoi, du logiciel au matériel informatique en passant par les politiques et les procédures particulières (que les employés ou les clients doivent suivre). Dans bien des cas, les mesures de protection sont composées d'un ensemble de ces éléments.

La suite du présent guide donne des conseils sur la façon dont votre entreprise peut mettre sur pied un processus de cybersécurité solide comportant l'identification des menaces et des risques, l'établissement de mesures de protection et la mise en place des structures de gestion dont vous avez besoin pour maintenir vos protections à jour.

Questions de gestion

Les conseils de cette section en un clin d'œil :

- Élaborez et mettez en œuvre un plan de cybersécurité qui décrit clairement les pratiques exemplaires pour tous les employés;
- Attribuez la responsabilité de la cybersécurité de votre entreprise à au moins un employé, et assurez-vous de lui fournir des instructions claires quant au travail à accomplir;
- Déterminez quels risques constituent des menaces faibles, moyennes et élevées pour votre entreprise – cette étape vous aidera à établir l'ordre de priorités;
- Assurez-vous que vos employés comprennent pourquoi la cybersécurité est importante pour eux et votre entreprise;
- Si vous avez des préoccupations d'ordre juridique concernant la cybersécurité, n'hésitez pas à consulter des experts (p. ex. conseiller juridique);
- Expliquez à vos employés les politiques et les normes afin qu'ils comprennent pourquoi vous voulez qu'elles soient mises en place, à qui elles s'appliquent et les risques pour eux et pour l'entreprise s'ils ne les respectent pas;
- Il est facile de sous-estimer combien un bon plan de cybersécurité peut coûter, alors assurez-vous d'établir un budget réaliste.

3.1 Sensibilisation à la cybersécurité

Tenter de se maintenir à jour en matière de cybersécurité peut sembler une tâche insurmontable. Un bon point de départ serait la mise en place d'un programme de sensibilisation à la sécurité.

Un programme de sensibilisation à la sécurité est une façon pour vous et vos employés de demeurer informés sur les bonnes pratiques en matière de cybersécurité. Un tel programme peut être très simple et facilement mis au point par vous ou d'autres employés. En premier lieu, une formation de base doit être donnée au personnel. Avec le temps, le programme devrait s'élargir pour inclure des mises à jour et des rappels sur les politiques, les normes et les pratiques exemplaires. Votre plan de sensibilisation à la sécurité devrait comprendre une évaluation périodique en vue de mettre à jour les mesures de protection existantes dans votre entreprise et d'adopter de nouveaux moyens de protection (logiciels et matériel informatique) au besoin.

Un programme de sensibilisation à la sécurité peut être très simple et facilement mis au point par vous ou d'autres employés.

La formation et l'éducation du personnel sont essentielles à un système de cybersécurité solide. Choisissez des sujets simples, ciblés et concis. Les messages clés devraient être répétés, mais il est aussi important d'interagir avec le personnel de multiples façons afin d'éviter qu'ils passent inaperçus. Par exemple, un avis concernant les pourriels pourrait être renforcé par des courriels, des affiches et des réunions du personnel. Vous pourriez même compléter le tout avec des jeux-questionnaires, des concours et des récompenses périodiques pour que les employés continuent à s'intéresser et à participer.

Questions de gestion

3.2 Définition des rôles et des responsabilités

Vous devriez nommer au moins une personne responsable de la cybersécurité dans votre entreprise. Cette personne aurait les responsabilités suivantes :

- S'informer sur les menaces, les tendances et les options de sécurité;
- Planifier, acquérir et mettre en œuvre des mesures de sécurité;
- Aider les autres membres du personnel à comprendre les politiques et les pratiques exemplaires en matière de cybersécurité;
- Mettre à exécution les politiques et les pratiques exemplaires en matière de cybersécurité avec l'aide de la direction;
- Maintenir les mesures de sécurité utilisées dans votre entreprise et les mettre à jour.

Même si une personne ou un groupe bien déterminé est responsable de la cybersécurité, leur succès dans une entreprise, quelle qu'en soit la taille, dépend du soutien de la direction. Le soutien que vous devez fournir dépend de la taille de l'entreprise, mais tous les gestionnaires sont responsables des éléments suivants :

- De donner des directives à tous les employés sur l'importance de la cybersécurité en tant qu'élément des activités professionnelles, d'inclure des politiques afin de décrire la responsabilisation à l'égard de la cybersécurité;
- D'appuyer et de surveiller les projets de cybersécurité;
- De consulter des experts, comme des conseillers juridiques, au sujet des obligations externes, par exemple, à l'égard d'une loi fédérale ou provinciale.

3.3 Élaboration de politiques et de normes

L'établissement des normes et des politiques rigoureuses en matière de cybersécurité, permettra aux employés de savoir comment se conduire.

Une *politique* en matière de sécurité est un document qui explique ce que les employés peuvent ou ne peuvent pas faire en matière de cybersécurité. Les politiques sur l'utilisation d'Internet, sur l'utilisation des médias sociaux et sur l'utilisation acceptable en sont des exemples. Une politique sur l'utilisation acceptable pourrait stipuler que « vous ne pouvez pas brancher un ordinateur personnel au réseau de l'entreprise » ou que « lorsque vous accédez au réseau de l'entreprise de chez vous, vous devez utiliser les outils de sécurité fournis ».

Une politique en matière de sécurité est un document qui explique ce que les employés peuvent ou ne peuvent pas faire en matière de cybersécurité.

Une norme est un document qui explique comment une tâche particulière doit être effectuée. Les normes s'appliquent le plus souvent à la mise en place de systèmes techniques et à leur utilisation.

Questions de gestion

Les politiques en matière de cybersécurité n'ont pas à être longues ni compliquées. Elles sont cependant essentielles pour aider vos employés à comprendre leurs rôles et responsabilités.

Une *norme* est un document qui explique comment une tâche particulière doit être effectuée. Les normes s'appliquent le plus souvent à la mise en place de systèmes techniques et à leur utilisation. Par exemple, une norme relative aux mots de passe décrirait exactement ce qu'un mot de passe acceptable peut et ne peut pas comprendre, sa longueur et la fréquence à laquelle il doit être changé.

Vous souhaiterez sans doute rédiger vous-même vos propres politiques en matière de cybersécurité, car elles doivent être précises et peuvent changer avec le temps. Et, vraisemblablement, certains domaines vous préoccuperont particulièrement.

Lorsque seront élaborées et utilisées des normes et des politiques en matière de cybersécurité :

1. Commencez avec une politique générale, mais relativement simple pour établir clairement les principes et les règles en matière de cybersécurité de votre entreprise;
2. Relevez les normes existantes et adaptez-les à certaines questions de cybersécurité ou de technologies de l'entreprise ou rédigez vos propres normes;
3. Expliquez les normes et les politiques aux membres du personnel afin qu'ils comprennent ce qui justifie les règles, à qui elles s'appliquent et les conséquences rattachées au non-respect de ces politiques;
4. Lorsque la politique initiale en matière de cybersécurité et les normes connexes seront appliquées, vous souhaiterez peut-être les revoir et ajouter des informations plus détaillées et spécifiques comme celles qui sont décrites dans diverses sections du présent guide. Par exemple, des détails au sujet de l'utilisation des médias sociaux si votre entreprise le temps sera peut-être venu d'envisager l'élaboration de politiques de soutien ciblées, comme celles qui sont décrites dans diverses sections du présent guide.

3.4 Planification de la sécurité

Selon une étude réalisée en 2012, 83 % des petites et moyennes entreprises ne disposent pas d'un plan de cybersécurité.[1] La mise au point d'un plan de cybersécurité devrait être une priorité pour toute entreprise. Un plan de cybersécurité déterminera les biens qui doivent être sécurisés, les menaces et les risques qui doivent être ciblés et les mesures de protection à mettre en place — tout cela selon un ordre de priorités.

Voici quelques étapes à suivre pour vous aider à préparer un plan de cybersécurité pour votre entreprise :

1. Remplissez l'outil d'auto-évaluation de l'état de cybersécurité à l'annexe A du présent guide. Vous mettrez ainsi en lumière les lacunes et les options relatives à la cybersécurité dans votre entreprise;
2. Dressez la liste de tous les biens de l'entreprise (comme les ordinateurs et l'information professionnelle) et déterminez leur importance et leur valeur pour l'entreprise;

[1] Étude nationale sur les petites entreprises, 2012, *NCSA/Symantec National Small Business Study*.

Questions de gestion

3. Discutez des menaces à la cybersécurité avec les employés ou des experts externes (au besoin) et déterminez quels biens risqueraient de subir un dommage si l'une ou plusieurs de ces menaces se concrétisaient;
4. Classez les risques par priorité selon l'échelle : élevé, moyen, faible;
5. Avec l'aide d'employés ou d'experts externes, déterminez ce qui peut être fait pour réduire ces risques;
6. Évaluez les menaces, les risques et les mesures de protection possibles, et décidez ce qui peut être fait et ce qui devrait être fait pour améliorer la cybersécurité au cours de l'année. Souvent, une amélioration peut être réalisée conjointement avec une autre afin de réduire l'ensemble des coûts. Par exemple, si vous êtes en train d'installer un pare-feu pour votre réseau, il pourrait inclure des options visant à bloquer les logiciels malveillants et les pourriels;
7. Fixez des échéances accessibles pour toutes les tâches liées à la cybersécurité et toutes les mesures de protection que vous prévoyez acheter;
8. Déterminez les ressources qui seront nécessaires pour mettre le plan en œuvre au cours de la première année, notamment les gens, le temps et l'argent;
9. Énumérez les problèmes qui pourraient nuire à votre plan (comme un manque de personnel ou un budget insuffisant);
10. Commencez à mettre le plan en œuvre;
11. Répétez l'étape 3, évaluation des menaces, au moins une fois par année.

Prenez note de tous les changements dans le plan et informez-en toutes les parties concernées (comme les fournisseurs) afin d'éviter la confusion. Par exemple, si vous avez engagé un expert pour vous aider à installer un pare-feu et que vous vous rendez compte que les pourriels sont devenus une priorité plus urgente, vous devrez peut-être modifier votre plan en ciblant les pourriels ou en incorporant le blocage des pourriels au pare-feu.

Vous devriez également évaluer les progrès à chaque clôture d'exercice et faire les modifications nécessaires. Dans la plupart des cas, un plan de cybersécurité pluriannuel nécessitera chaque année des mises à jour afin d'être adapté aux priorités changeantes et aux ressources de l'entreprise.

Vous devriez également évaluer les progrès à chaque clôture d'exercice et faire les modifications nécessaires. Dans la plupart des cas, un plan de cybersécurité pluriannuel nécessitera chaque année des mises à jour afin d'être adapté aux priorités changeantes et aux ressources de l'entreprise.

Questions de gestion

3.5 Budget de cybersécurité

Un plan de cybersécurité efficace coûte de l'argent et il faut en tenir compte lorsque vous établissez vos plans d'activités et vos budgets annuels. Heureusement, il est possible d'obtenir des services, des outils et des conseils gratuits. En outre, les politiques ou les documents internes peuvent souvent être créés au sein l'entreprise, à coût minime.

Mais certains éléments clés, comme des mesures de protection, devront être achetés et pourront aussi comporter des frais d'abonnement annuel. Par exemple, contrairement à un logiciel que vous payez typiquement une fois, un abonnement à un logiciel de lutte aux programmes malveillants devra être renouvelé chaque année moyennant des frais.

Afin d'éviter les surprises, mieux vaut prévoir :

1. Le coût de départ des outils de sécurité ainsi que les frais de mise à niveau et de mise à jour;
2. Les frais rattachés au soutien, aux conseils ou à la formation;
3. Les fonds de prévoyance.

Les fonds de prévoyance sont importants pour composer avec les urgences imprévues (comme une infection par un programme malveillant).

Dans certains cas, votre assurance pourrait couvrir les pertes dues à un incident lié à la cybersécurité. Il est important d'en discuter à l'avance avec votre assureur.

Sécurité sur le Web

Les conseils de cette section en un clin d'œil :

- Limiter les genres de sites Web dont vous permettez l'accès à vos employés vous aidera à exclure ceux qui pourraient détériorer votre réseau;
- Informez vos employés des logiciels qu'ils peuvent installer en toute sécurité et demandez-leur d'obtenir la permission avant de télécharger de nouveaux programmes;
- Lorsqu'un tiers demande des renseignements personnels ou sur l'entreprise, vérifiez s'il est sécuritaire de lui transmettre ces renseignements;
- Rédigez une politique sur l'utilisation d'Internet à l'intention du personnel et affichez-la à un endroit accessible pour tous où ils pourront la consulter;
- Définissez les règles relatives aux types de renseignements que vos employés peuvent partager en ligne au sujet de l'entreprise, et aux endroits où ils peuvent le faire;
- Donnez des instructions qui préciseront si vos employés peuvent ou non utiliser leur messagerie professionnelle pour s'inscrire à des sites de médias sociaux et à des bulletins;
- Envisagez l'instauration d'une politique d'entreprise sur les médias sociaux qui permettra aux employés de savoir ce qu'ils doivent ou ne doivent pas afficher en ligne;
- Mettez à niveau tous vos logiciels opérationnels lorsque vous recevez des avis à cet égard afin que tous les correctifs de sécurité soient à niveau;
- Exigez de vos employés qu'ils aient des mots de passe complexes contenant des lettres, des chiffres et des symboles afin qu'ils soient plus difficiles à compromettre pour les cybercriminels;
- Méfiez-vous toujours des appels téléphoniques, des courriels et des autres communications provenant d'une source inconnue.

4.1 Protection des renseignements personnels et professionnels en ligne

Pour leur propre sécurité et pour celle de votre entreprise, les employés devraient protéger leurs renseignements personnels et professionnels lorsqu'ils sont en ligne. Les renseignements personnels et ceux de l'entreprise comprennent des éléments privés ou confidentiels, comme des noms complets, des numéros d'assurance sociale, des renseignements bancaires sur un compte ou autres et des mots de passe.

Il est important que tous les employés comprennent pourquoi il est essentiel de protéger les renseignements en ligne. Les criminels qui veulent nuire à votre entreprise ou la voler commencent souvent par amasser des renseignements personnels ou professionnels afin d'accéder à vos systèmes informatiques et à l'information confidentielle.

Voici quelques conseils simples aux employés :

- Utilisez uniquement des sites Web légitimes et fiables lorsque vous utilisez les ordinateurs de l'entreprise ou que vous travaillez avec des renseignements professionnels;
- Avant de transmettre des renseignements personnels à qui que ce soit, vérifiez qu'il s'agit d'une source sûre (par exemple, une banque ne traiterait pas de questions personnelles par courriel; il pourrait donc être sage d'appeler votre banque si vous recevez ce genre de courriel);
- Si quelqu'un veut obtenir des renseignements personnels, demandez-lui pourquoi ils sont nécessaires;

- Si la réponse ne semble pas satisfaisante, ne les donnez pas ou demandez à parler à son superviseur pour obtenir davantage de détails;
- N'enlevez ou ne désactivez jamais les mesures de protection mises en place dans les réseaux et les ordinateurs de l'entreprise (comme l'antivirus).

4.2 Navigation Web sécuritaire

Les recherches, la collaboration, la communication avec des clients, les achats et bien d'autres activités professionnelles se font par Internet. Le Web recèle cependant de nombreuses menaces pour votre entreprise, à commencer par celles qui existent dans l'accomplissement d'une simple tâche quotidienne : la navigation.

La navigation sécuritaire exige un ensemble de mesures de protection et de pratiques de sécurité. Voici quelques étapes à suivre pour vous assurer que vous naviguez de façon sécuritaire :

1. Commencez par rédiger et publier une politique sur l'utilisation d'Internet qui explique clairement aux employés ce qu'ils peuvent et ne peuvent pas faire lorsqu'ils utilisent les systèmes de l'entreprise pour se connecter à Internet. Vous trouverez des exemples de politique sur l'utilisation d'Internet en ligne;
2. Donnez à vos employés une formation sur le contenu de votre politique sur l'utilisation d'Internet;
3. Encouragez la sensibilisation continue à la sécurité en communiquant régulièrement avec les employés au sujet des pratiques de navigation sécuritaire;
4. Expliquez aux employés comment vérifier l'adresse URL des sites Web qu'ils se préparent à visiter afin qu'ils évitent de visiter des sites dangereux (voir les conseils dans l'encadré qui suit);
5. Installez un outil de classification des sites en tant qu'extension du navigateur sur les ordinateurs des utilisateurs (Figure 2). Cela les aidera à reconnaître les sites sécuritaires.

Figure 2 : Modèle d'écran d'un outil de classification de sites Web

Comment reconnaître un lien suspect dans une page Web

Lorsque vous placez votre curseur sur un lien, l'adresse URL de destination apparaît, soit dans une petite fenêtre qui s'ouvre au-dessus du lien ou au bas de la fenêtre de navigation. Essayez cela avant de cliquer sur un lien et faites les vérifications suivantes :

- Si le texte relié est une URL, comparez-la avec la véritable destination. Les cybercriminels utilisent souvent un texte du genre « connectez-vous à www.mabanque.com pour mettre à jour les renseignements sur votre compte », mais la véritable destination est un site semblable hébergé en un autre lieu, comme www.mafaussebanque.com;
- Vérifiez si des URL sont semblables à celles de sites que vous connaissez, mais légèrement différentes (p. ex. Goggle.com ou Google1.com à la place de Google.com). Cette technique est souvent utilisée pour tromper la confiance des gens lorsqu'ils visitent certains sites. Dans bien des cas, les faux sites sont une imitation presque identique de l'original qu'ils copient;
- Méfiez-vous toujours des URL que vous ne reconnaissez pas;
- N'oubliez pas que des images, aussi bien que des textes, peuvent être liées; avant de cliquer sur une image, soyez donc aussi vigilant que si vous cliquiez sur un texte;
- Si vous avez des doutes, copiez l'URL et collez-la dans un moteur de recherche pour identifier le site sans le visiter.

4.3 Médias sociaux

Les sites de réseaux sociaux, comme Facebook, Twitter et LinkedIn peuvent s'avérer de formidables outils pour entrer en contact avec des clients potentiels et renforcer vos relations avec ceux que vous avez déjà. Cependant, les sites et les services des réseaux sociaux constituent pour les cybercriminels une façon de plus en plus populaire d'essayer d'accéder à vos renseignements personnels ou professionnels afin de pirater vos systèmes informatiques personnels ou ceux de votre entreprise.

Si votre entreprise utilise les sites de réseaux sociaux à des fins professionnelles ou publicitaires, vous devrez choisir un ou plusieurs employés et autoriser uniquement cet employé ou ces employés à placer du contenu au nom de l'entreprise.

Votre politique sur l'utilisation d'Internet devrait traiter des réseaux sociaux et donner des directives claires aux employés. Voici quelques questions sur les réseaux sociaux dont vous devriez tenir compte :

- Établissez clairement quels renseignements concernant votre entreprise peuvent être affichés en ligne, et qui peut le faire;
- Évitez d'inclure des renseignements de nature délicate à votre profil d'entreprise ou à vos messages;
- Soyez prudents lorsque vous utilisez des applications dans les sites de réseaux sociaux. Beaucoup proviennent de tiers et pourraient ne pas être sécuritaires. Vérifiez toujours le fournisseur de l'application en premier lieu;
- Sur les médias sociaux, méfiez-vous toujours de messages vous demandant des renseignements de nature délicate sur l'entreprise ou vos employés et leurs familles;

- Réfléchissez avant d'afficher un message! Ce que vous affichez sur les médias sociaux est généralement permanent. Vous pourriez, un jour, changer d'idée sur une chose que vous avez dite en ligne, mais il sera impossible de l'éliminer ou de la modifier.

Au travail, il est probable que vos employés utilisent les médias sociaux pour des raisons personnelles, tant pour rester en contact avec leurs amis et leur famille que pour suivre l'actualité. Il est impératif que les employés suivent des lignes directrices similaires pour protéger leurs propres renseignements sur les réseaux sociaux, de même que sur les réseaux et les appareils de votre entreprise.

Voici quelques conseils supplémentaires concernant l'utilisation des médias sociaux par les employés à des fins personnelles :

- Les criminels s'intéressent aux renseignements que vous affichez. Afin que votre entreprise demeure sûre, veillez à utiliser les contrôles de confidentialité du site et à ne pas répondre aux demandes de gens que vous ne connaissez pas;
- Revoyez les politiques de confidentialité du site de réseautage social et demeurez à jour (la plupart font des mises à jour fréquentes) et modifiez vos réglages de renseignements personnels de façon appropriée;
- Ne révélez jamais le lieu précis où vous êtes en ligne.

4.4 Ingénierie sociale

L'ingénierie sociale est une pratique employée par des cybercriminels pour extorquer des renseignements sur une entreprise ou ses systèmes informatiques en manipulant leurs utilisateurs.

Les cybercriminels emploient l'ingénierie sociale pour recueillir l'information dont ils ont besoin pour commettre une fraude ou accéder aux systèmes informatiques. Ils semblent sérieux et honnêtes. Ils peuvent même vous dire qu'ils ont un lien légitime avec votre entreprise (p. ex. en tant que client ou par l'entremise d'une autre entreprise) et offrir des « preuves ». Certains se font passer pour un représentant du gouvernement. Ils peuvent demander des renseignements, comme des numéros de téléphone ou de l'information sur un compte, ou vous demander d'ouvrir des courriels avec des pièces jointes ou de visiter des sites Web particuliers. Ce n'est que plus tard que les victimes se rendent compte que ces demandes étaient une duperie et qu'elles ont été manipulées.

Ces tactiques sont populaires parce qu'elles fonctionnent. Il est important de vérifier à qui vous avez affaire avant de divulguer des renseignements personnels ou professionnels.

Soyez prudents. Protégez votre entreprise et vos employés en leur demandant d'agir de la façon suivante :

- Être sur leurs gardes lorsqu'ils reçoivent des appels téléphoniques, des visites ou des courriels de gens qui posent des questions sur des employés, leurs familles et sur des données professionnelles délicates. Une telle attitude devrait être renforcée dans le cadre d'un programme continu de sensibilisation à la sécurité;
- Demander à toutes les personnes qui font des demandes inhabituelles de confirmer leur identité à l'aide de documents officiels. En cas de doutes, demander l'aide d'un superviseur ou d'un collègue;

- Suivre les pratiques de sécurité à l'égard des courriels, du réseautage social et autres (telles que décrites tout au long du présent guide) et toujours protéger les renseignements personnels en ligne;
- Toujours rapporter les activités suspectes, notamment les tentatives d'ingénierie sociale, à un superviseur. Cela est particulièrement important si vous pensez que votre entreprise a été compromise;
- S'il est possible que votre entreprise ait perdu ou révélé des renseignements de nature délicate au cours d'un tel incident, ou si un modèle suspect de demandes circule, déterminez quels biens peuvent être à risque et prenez des mesures pour les protéger davantage. Par exemple, si vous avez des raisons de croire que quelqu'un a obtenu les renseignements bancaires de votre entreprise, avertissez votre banque immédiatement et demandez de l'aide pour protéger vos comptes;
- Envisager de signaler l'incident à la police;
- Prendre contact avec le Centre antifraude du Canada et demander des conseils ou faire un rapport.

En grande partie, la cybersécurité consiste à être vigilants lorsque des choses semblent « sortir de l'ordinaire ». Vos employés doivent toujours sentir qu'ils peuvent parler de questions, d'inquiétudes et d'observations relatives à la sécurité à une personne en position d'autorité (technique ou administrative) qui écoutera, consignera ce qui s'est produit et prendra les mesures appropriées.

4.5 Sécurité logicielle

La cybersécurité de votre entreprise est à la hauteur de celle des logiciels que vous utilisez. En fait, si vous protégez tous vos logiciels, un grand nombre de menaces à la sécurité sera réduit ou résolu.

Les logiciels peuvent comprendre :

- Des applications de bureautique;
- Des applications d'appareils mobiles;
- Des serveurs Web et des logiciels connexes;
- Des systèmes d'exploitation et davantage.

Les logiciels présentent parfois des problèmes (habituellement appelés « bogues ») qui risquent de les rendre non sécuritaires. Des attaquants peuvent exploiter ces bogues et ainsi, accéder à vos renseignements. Il arrive aussi qu'un logiciel transporte un programme *malveillant*.

Appliquez les mises à jour de sécurité à vos logiciels dès qu'elles sont offertes par le développeur.

Conseils pour maintenir la sécurité des logiciels :

- N'utilisez que des logiciels légitimes qui ont été testés et utilisés par d'autres; il peut s'agir d'un logiciel provenant de fournisseurs connus ou de développeurs indépendants qui pourraient même l'offrir gratuitement;
- N'utilisez pas de versions non autorisées d'un logiciel téléchargées illégalement au moyen de systèmes d'échange de fichiers, car ils sont souvent infectés par des programmes malveillants;

les logiciels copiés illégalement ne bénéficient pas du soutien des développeurs, ce qui signifie que votre entreprise ne peut s'attendre à aucune sorte de soutien technique si vous avez des problèmes;
- Limitez l'accès aux applications partagées uniquement aux personnes qui en ont vraiment besoin. Cette limite peut parfois être installée dans le logiciel même ou par l'entremise du système d'exploitation;
- Limitez le nombre d'employés ayant des privilèges administratifs à l'égard des logiciels, surtout pour les applications importantes et les mesures de protection. Votre entreprise deviendra alors moins vulnérable aux erreurs internes et aux attaques externes. Beaucoup d'attaquants ciblent les comptes d'utilisateur ayant des privilèges administratifs, car ils obtiennent ainsi un niveau de pouvoir élevé sur les logiciels et les systèmes;
- Il est extrêmement important d'appliquer les mises à jour de sécurité (correctifs) à vos logiciels, et ce, dès qu'ils sont disponibles. Certains avis concernant les logiciels sont automatisés, mais dans d'autres cas, une visite régulière au site du fournisseur s'impose.

4.6 Hébergement sécuritaire et sécurité des entreprises sur le Web

Si le site Web de votre entreprise n'est pas correctement sécurisé, il pourrait être facilement compromis, ce qui pourrait mener au vandalisme, à des perturbations de service ou au vol de données des clients ou de l'entreprise. Tout cela peut avoir des conséquences graves.

Les sites Web varient d'une entreprise à l'autre, mais certains conseils de base doivent être suivis :

1. Si vos sites Web sont hébergés entre vos murs ou dans des serveurs qui appartiennent à votre entreprise :
   - Accordez l'accès uniquement aux employés autorisés;
   - Appliquez tous les correctifs disponibles et pertinents aux systèmes d'exploitation du serveur Web et aux autres logiciels actifs pour aider à résoudre les problèmes connus;
   - Planifiez des sauvegardes régulières des systèmes de votre entreprise sur un serveur qui se trouve en un lieu différent;
   - Activez les journaux du serveur et demandez à la personne qui s'occupe du ou des serveurs d'examiner régulièrement les journaux et de garder l'œil ouvert sur les activités suspectes.
2. Si votre entreprise utilise un service d'hébergement Web, assurez-vous que les responsables de ce service disposent d'un plan de sécurité et :
   - Qu'un balayage des serveurs Web et de votre site est effectué régulièrement pour trouver les problèmes potentiels et ensuite, les corriger afin que votre serveur et votre site soient protégés;
   - Que votre site Web et tous les systèmes sont surveillés contre les intrusions ou les tentatives de vandalisme;
   - Que votre site Web est protégé des intrusions et des perturbations;
   - Que le service sera restauré sur votre site en cas de panne ou de perturbations provoquées par des cybercriminels.
3. N'affichez pas d'adresses de courriel personnelles sur le site Web de votre entreprise, car des polluposteurs et d'autres les utiliseront (p. ex. pour faire de l'hameçonnage). Utilisez des comptes génériques, comme ventes@nomdelentreprise.com ou soutien@nomdelentreprise.com.
4. Soyez prêt au cas où le site Web de votre entreprise serait compromis. Vous pourriez devoir réduire votre service, recourir à un serveur de sauvegarde ou à un fournisseur de service ou même mettre temporairement votre site Web hors ligne. Examinez toutes ces possibilités avant que survienne un incident lié à la sécurité afin que tous dans l'entreprise sachent ce qu'il faut faire.

Sécurité sur le Web

4.7 Programmes malveillants

Un programme malveillant est un logiciel créé et distribué dans le but de causer des dommages ou de voler des renseignements. Il est conçu pour s'infiltrer dans un système d'exploitation et éviter les mesures de protection. Il peut s'avérer impossible de le détecter ou de l'éliminer sans le recours à une expertise ou à des outils spécialisés. Il en existe pour tous les systèmes de traitement de l'information qui peuvent être utilisés dans votre entreprise, par exemple, des ordinateurs de table ou portatifs, des téléphones intelligents et des tablettes.

Le genre de programme malveillant le plus courant est le virus. Un virus est un programme qui se copie lui-même d'un système à un autre et qui infecte chaque ordinateur au passage. Lorsqu'un virus a infecté le système d'une entreprise, il peut supprimer ou corrompre des dossiers, voler des données ou même (en de rares cas) endommager le matériel informatique. Il peut provenir de pièces jointes à un courriel, de téléchargements d'un site Web ou de disques infectés utilisés par plusieurs personnes.

De nombreux autres types de programmes malveillants existent, mais ils ont tous le même objectif : recueillir et voler des renseignements de nature délicate (p. ex. des mots de passe) et les transmettre à leur initiateur sans que les utilisateurs du système en aient connaissance.

Utilisez un logiciel anti-programme malveillant pour balayer tous les fichiers entrants et bloquer tout ce qui est suspect ou qui contient un programme malveillant.

La lutte aux programmes malveillants est parfois difficile, mais vous pouvez neutraliser bon nombre de menaces avec un logiciel anti-programmes malveillants qui balaie les dossiers entrants (p. ex. les pièces jointes à un courriel) et les bloque si la présence d'un tel programme est suspectée ou confirmée. Le même logiciel cherchera les infections déjà existantes, avertira les utilisateurs et proposera des options de nettoyage. Certains programmes malveillants ne peuvent être éliminés sans l'aide d'un expert de la sécurité. La prévention est toujours la meilleure solution. Installez votre protection contre les programmes malveillants avant d'être infecté.

La plupart des logiciels anti-programmes malveillants modernes couvrent tous les genres de programmes malveillants décrits dans cette section, mais certains sont toujours appelés « logiciels antivirus ». Avant d'acheter ou d'utiliser des outils de lutte contre les programmes malveillants, vérifiez le genre de programmes malveillants qu'ils combattent et voyez à quel intervalle le logiciel est mis à jour. Plus les mises à jour sont fréquentes, mieux c'est, car de nouveaux programmes malveillants émergent toutes les heures.

Votre entreprise peut aussi avoir besoin d'un pare-feu pour bloquer les connexions à des sites Web malveillants et arrêter certaines formes de programmes avant qu'ils soient téléchargés ou introduits par l'entremise d'un courriel.

L'installation d'un logiciel anti-programmes malveillants et d'un pare-feu est un premier pas formidable pour renforcer la cybersécurité de votre entreprise. De bonnes habitudes chez les employés sont aussi essentielles. Tous les employés doivent recevoir une formation sur la sensibilisation à la sécurité et l'entreprise doit leur fournir des politiques en matière de sécurité qui expliquent en quoi consistent leurs responsabilités. Par exemple, ils devraient être avertis qu'il leur est interdit de trafiquer ou de désactiver les mesures de protection, y compris les logiciels anti-programmes malveillants.

Sécurité sur le Web

Voici certaines choses que vous devriez demander à vos employés de surveiller :

- Les avertissements concernant des sites Web ou des courriels signalés comme étant potentiellement dangereux;
- Rapporter (p. ex. à un superviseur ou à quelqu'un du soutien technique) toutes les alertes provenant du logiciel anti-programmes malveillants dans leur ordinateur de travail, y compris les alertes qui indiquent que le logiciel n'est plus à jour ou qu'il a repéré un fichier suspect;
- Ne jamais transmettre de courriels ou de fichiers suspects aux autres personnes de votre entreprise.

4.8 Pratiques exemplaires en matière d'authentification

L'authentification est une pratique de sécurité qui a pour but de vérifier qu'un utilisateur est bien la personne qu'il prétend être avant de lui accorder l'accès à des systèmes ou à des services particuliers de votre entreprise.

4.8.1 Mots de passe

Les mots de passe sont largement utilisés pour protéger l'accès aux renseignements professionnels et aux outils en ligne, mais si les employés ne sont pas prudents, d'autres personnes peuvent utiliser leurs mots de passe afin d'accéder à des dossiers et à des renseignements cruciaux.

Voici plusieurs problèmes courants relatifs à l'utilisation des mots de passe en entreprise :

- Les employés notent leurs mots de passe et les placent à des endroits où d'autres peuvent les copier ou les divulguent tout simplement à des tiers. Dans les deux cas, la perte de contrôle de ces mots de passe fait en sorte qu'il est impossible de garantir que la personne qui accède aux systèmes est autorisée à le faire;
- Les employés utilisent des mots de passe faibles, faciles à deviner, ce qui rend possible l'accès d'autres personnes à des systèmes ou à des renseignements de nature délicate;
- Ils utilisent le même mot de passe pour plusieurs systèmes ou services de sorte que si l'un d'entre eux est compromis, tous les autres sont à risque;
- Ils ne changent pas leurs mots de passe régulièrement.

Adoptez une politique rigoureuse en matière de mots de passe décrivant les règles qui doivent s'appliquer à ceux qui sont utilisés dans votre entreprise. Les directives suivantes devraient en faire partie :

- Évitez les mots communs, comme « mot de passe » ou « connexion »;
- Évitez les séquences de nombres simples, comme « 1234 »;
- Évitez les noms propres faciles à deviner, comme le prénom d'un enfant;
- Créez des mots de passe comptant au moins huit caractères — plus le nombre de caractères est élevé, plus un mot de passe est sécuritaire;
- Créez un mot de passe fort en incluant une combinaison des éléments suivants :
  - Lettres majuscules;
  - Lettres minuscules;
  - Chiffres;
  - Caractères spéciaux (p. ex. : !, $, # ou %).

Expliquez à vos employés que les mots de passe forts sont importants pour la sécurité de l'entreprise. Encouragez-les à suivre ces conseils pour protéger leurs mots de passe :

- Garder leurs mots de passe confidentiels;
- Changer leurs mots de passe régulièrement. Votre entreprise devrait exiger ce changement tous les trois mois;
- Éviter d'utiliser le même mot de passe pour plusieurs comptes ou systèmes.

Vous pourriez aussi envisager l'utilisation d'un gestionnaire de mots de passe (un programme qui génère et stocke des mots de passe aléatoires) qui créera des mots de passe encore plus forts à l'usage des employés.

4.8.2 Phrases passe

Si vous avez besoin d'une sécurité renforcée, pensez à employer une phrase passe plutôt qu'un mot de passe. Une phrase de passe est une séquence complète de mots. Par exemple, à la place du mot de passe « Bonm0tdepasse », la phrase de passe « !esuisravi7unbonm0t2passe! » serait beaucoup plus difficile à deviner.

Une phrase de passe sous forme d'acronyme réduit le nombre de clés à employer. Par exemple, « Je suis heureux d'être allé en vacances en janvier, car j'aime le soleil! » deviendrait « JSHDEAEVEJCJALS! ». Même ce genre d'acronymes est plus sécuritaire qu'un mot de passe ordinaire, car il est plus long, plus complexe et imprévisible, ce qui le rend difficile à deviner — même avec les outils logiciels que les cybercriminels utilisent.

Il existe de nombreux outils en ligne gratuits que vous pouvez utiliser pour tester la force relative des mots de passe. Ces divers outils peuvent produire des résultats légèrement différents, mais si vous en essayez plusieurs, vous aurez une bonne idée de la force du mot de passe que vous avez choisi.

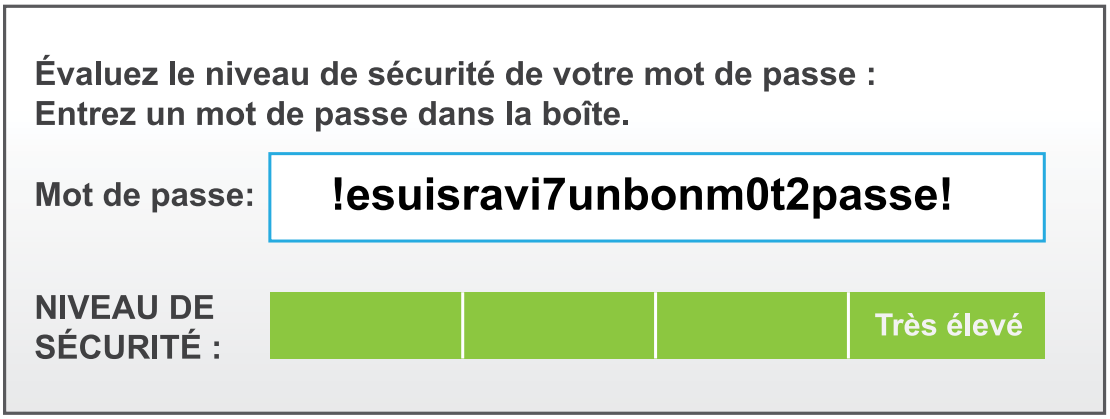


Figure 3 : Exemple de la force d'une phrase passe

4.8.3 Authentification à deux facteurs

L'authentification à deux facteurs (2FA) est une pratique de sécurité qui ajoute un moyen d'identification supplémentaire, ce qui peut rendre le système d'une entreprise beaucoup plus sécuritaire.

Le « premier facteur » est une chose que la personne connaît (p. ex. un mot de passe) et le deuxième facteur est un élément à ajouter pour confirmer l'identité de la personne. Le deuxième facteur peut être une chose que possède l'utilisateur (p. ex. ses empreintes digitales, maintenant utilisées à de nombreux postes frontaliers) ou autre chose, comme un mot de passe à usage unique. À la différence du mot de passe ordinaire, le mot de passe à usage unique ne peut pas être deviné et, comme son nom le suggère, ne peut pas être utilisé à nouveau.

Le mot de passe à usage unique est généré par l'utilisateur avec une application sécuritaire (p. ex. son téléphone intelligent) ou un périphérique dédié (souvent appelé jeton). Les deux sont portatifs et peuvent être utilisés au besoin. Lorsqu'il est combiné à un nom d'utilisateur ordinaire et à un mot de passe, le mot de passe à usage unique renforce grandement la sécurité de l'authentification.

Figure 4 : Exemple d'un mot de passe à usage unique qui montre que ce dernier expirera dans 17 secondes

Il est fortement recommandé d'installer des authentifications à deux facteurs dans votre entreprise, surtout pour la protection des systèmes et des renseignements essentiels. Vous pouvez commencer avec des services simples, comme les courriels Web ou les transactions bancaires pour en saisir le fonctionnement et par la suite, en élargir l'utilisation à mesure que le permettent votre temps et votre budget.

Sécurité des points de vente (PDV)

Les conseils de cette section en un clin d'œil :

- Assurez-vous que votre système de PDV est protégé par un pare-feu;
- Mettez en place un chiffrement robuste pour toutes les données transmises;
- N'utilisez pas le nom d'utilisateur et le mot de passe par défaut fournis par le fabricant;
- Accordez un accès aux données des clients uniquement aux employés qui en ont absolument besoin;
- Assurez-vous que tous les logiciels anti-programmes malveillants sont à jour, car les mises à jour de sécurité pour combattre les nouveaux genres de programmes malveillants sont fréquentes;
- Si vous avez des préoccupations concernant la sécurité de votre système de PDV, vous pouvez communiquer avec votre fournisseur de services.

Votre entreprise a sans doute recours aux systèmes de points de vente (PDV) électroniques pour exécuter ses transactions financières. Les consommateurs s'attendent maintenant à profiter de la commodité des PDV pour effectuer des transactions instantanées avec leurs cartes de débit ou de crédit, ce qui les rend essentiels à votre entreprise.

Les systèmes de PDV peuvent constituer un autre moyen d'accéder à vos réseaux informatiques et il est extrêmement important de les protéger. Les cybercriminels peuvent pirater les systèmes de PDV afin de voler des numéros de cartes de paiement et les numéros d'identification personnels (NIP) qui y sont associés, et les utiliser pour accéder aux comptes de vos clients.

Vous pouvez prendre certaines mesures pour améliorer la sécurité de vos PDV et contribuer à la protection de vos clients et de votre entreprise :

- Veillez à ce que votre système de PDV soit protégé par un pare-feu. Un pare-feu est un contrôle de sécurité utilisé pour restreindre la transmission de données qui entrent et sortent du réseau. Votre fournisseur de services Internet peut inclure un pare-feu au routeur ou à d'autres périphériques ou logiciels qu'il vous procure, mais il est important de le vérifier. S'il ne vous en fournit pas, vous devrez en acheter un;
- Mettez en place un chiffrement robuste pour toutes les données que vous transmettez (p. ex. les données des détenteurs de carte) entre votre système de PDV et le fournisseur de service de PDV. Ce dernier devrait installer cette fonction par défaut. Demandez de l'aide à votre fournisseur de service de PDV ou à un conseiller en cybersécurité (ayant l'expérience des PDV) si vous n'êtes pas certain de ce qu'il faut faire;
- N'utilisez pas le nom d'utilisateur ni le mot de passe par défaut de votre système de PDV (expédié avec le système). Les cybercriminels utiliseront ces authentifiants pour accéder à votre système. Utilisez plutôt un nouveau nom d'utilisateur et un nouveau mot de passe, unique à votre entreprise;
- Limitez toujours l'accès aux données des clients aux employés qui en ont besoin et qui ont l'autorisation voulue;
- Maintenez les logiciels anti-programmes malveillants à jour.

Sécurité du courrier électronique

Les conseils de cette section en un clin d'œil :

- Mettez en place un filtre antipourriel – cette étape vous permettra de vous débarrasser de la plupart des courriels nuisibles, envoyés par les cybercriminels;
- Vous ne devriez pas cliquer sur des liens non vérifiés ou suspects — le simple fait de cliquer sur un lien permet de transmettre de l'information délicate qu'un cybercriminel pourrait utiliser pour vous faire du tort ou en faire à votre entreprise;
- Maintenez les courriels de vos employés et les renseignements sur ces derniers confidentiels, car des renseignements sur un membre de votre entreprise pourraient servir à nuire à vos employés ou à votre entreprise;
- Activez un format HTTPS, qui chiffre les données et empêche les cybercriminels d'accéder aux renseignements qui se trouvent dans le navigateur que vous utilisez pour les courriels Web.
- Établissez des normes strictes sur les mots de passe des comptes courriel (personnels ou de l'entreprise) utilisés au travail;
- Lorsque cela est possible, utilisez des comptes courriel génériques (comme info@nomdelentreprise.com) pour les adresses de courriel qui sont affichées à des endroits publics (comme votre site Web ou les médias sociaux);
- Ne transférez pas de courriels possiblement malveillants à d'autres employés.

Beaucoup de préoccupations en matière de sécurité ont fait leur apparition en raison de l'adoption universelle du courrier électronique, par exemple, les pourriels, l'hameçonnage et l'échange non sécuritaire de renseignements confidentiels. Toutes ces choses peuvent avoir un effet négatif sur votre entreprise.

6.1 Pourriels

Les pourriels sont des courriels envoyés à une personne sans sa permission et sans qu'elle en ait fait la demande. Les pourriels représentent environ 69 % de tous les courriels transmis dans Internet.[1] Non seulement les pourriels contiennent-ils des liens qui peuvent faire du tort à votre entreprise si vous cliquez dessus, mais ils peuvent aussi ralentir vos réseaux, vos serveurs et vos ordinateurs, ainsi qu'accroître les coûts et réduire la productivité.

Les pourriels sont utilisés abondamment pour :

- Vous vendre un produit ou un service (très semblable au télémarketing, mais par courriel) et vous faire visiter des sites non sécuritaires d'où vous téléchargerez des programmes malveillants dans votre ordinateur;
- Vous convaincre de divulguer des renseignements confidentiels personnels ou professionnels (comme des mots de passe).

[1] http://www.symantec.com/security_response/publications/threatreport.jsp, en anglais seulement.

Sécurité du courrier électronique

Comment repérer les pourriels potentiels

Voici quelques façons de repérer les pourriels potentiels :
- Si vous ne reconnaissez pas l'expéditeur, soyez prudent;
- Chercher les fautes d'orthographe dans le corps du courriel; les fautes sont une astuce que les fraudeurs utilisent pour déjouer les filtres antipourriel (voir l'explication plus loin);
- Recherchez les formulations inhabituelles dans le message, elles peuvent suggérer que l'auteur n'est pas légitime.

Méfiez-vous toujours des courriels qui contiennent :
- Des offres qui semblent trop belles pour être vraies;
- Des invitations à cliquer sur un lien dans le message;
- Des demandes de renseignements personnels.

Les pourriels sont irritants et potentiellement dangereux pour votre entreprise. Mais il existe des façons de s'en protéger :

- Installez un filtre antipourriel qui bloquera la plupart des pourriels et laissera seulement passer les courriels légitimes. Si votre entreprise utilise un service de courrier électronique hébergé par une autre entreprise, demandez aux responsables quelle sorte de services antipourriel ils offrent. Si ces derniers ne fonctionnent pas bien, demandez un meilleur filtre antipourriel ou changez de fournisseur de service de courrier électronique;
- Gardez la liste des adresses courriel de vos employés confidentielle. Si vous devez transmettre une adresse de courriel à un tiers hors de votre entreprise, utilisez une adresse générique, comme aidealaclientele@nomdelentreprise.ca;
- Élaborez un ensemble de directives de base relatives aux courriels pour vos employés et veillez à ce que tous les employés les lisent et les mettent en application. Elles devraient comprendre les éléments suivants :
  - Ne jamais cliquer sur des liens figurant dans un pourriel, même s'il s'agit d'une offre de vous retirer d'une liste de distribution. C'est une ruse répandue pour inciter les gens à visiter des sites Web dangereux;
  - Ne jamais ouvrir de pièces jointes à des pourriels ou à des courriels suspectés d'en être;
  - Ne jamais écrire au polluposteur, et ce, pour quelque raison que ce soit, même pour déposer une plainte. Agir ainsi ne fera que confirmer la validité de votre adresse et aura pour conséquence un nombre accru de pourriels;
  - Supprimez les pourriels si vous êtes certains qu'ils sont illégitimes. Dans le doute, demandez l'aide d'un superviseur ou d'un membre du soutien technique. En général, si votre entreprise n'a pas de personnel de soutien technique disponible, il vaudrait mieux prendre contact avec le fournisseur de service de courrier électronique. Dans les pires cas, si vous suspectez un risque important pour votre entreprise, vous devriez prendre contact avec les autorités qui figurent dans la liste de l'annexe C.

Sécurité du courrier électronique

6.2 Hameçonnage

L'hameçonnage est une forme particulière de pourriel qui vous cible en simulant un message provenant d'une banque, d'un ministère ou d'une organisation en vue de vous inciter à divulguer des renseignements confidentiels qui pourraient être utilisés à des fins criminelles.

Ces messages sont souvent rédigés de sorte qu'ils semblent utiles ou porteurs de « bonnes nouvelles » (Figure 5) afin de vous inciter à avoir confiance en l'expéditeur et à suivre les directives du courriel. Dans d'autres cas, ils essaient de vous effrayer et de vous faire réagir (p. ex. « … nous fermons votre compte bancaire. Cliquez ici pour corriger la situation immédiatement. »).

Parce que ces messages semblent souvent provenir d'organisations réelles (les vrais logos, les couleurs, la disposition et les polices habituelles figurent parfois dans le message), vous pouvez avoir de la difficulté à voir qu'ils sont illégitimes. Dans presque tous les cas, le message comportera l'URL d'un site Web (un lien), sur lequel les auteurs souhaitent que vous cliquiez, et *une demande de renseignements confidentiels.*

Ce qu'il faut faire des courriels potentiellement criminels

Si vous recevez des courriels offensants, comportant des insultes ou potentiellement criminels (qu'ils aient ou non l'apparence de pourriels) ou si vous pensez que des criminels vous demandent des renseignements personnels, vous devriez sauvegarder le message (**n'envoyez pas** ces courriels à quelqu'un d'autre) et en parler à votre superviseur ou à un membre du personnel de soutien des TI. Un responsable pourrait vous demander une copie du message afin d'aider les autorités dans leurs prochaines enquêtes — c'est la raison pour laquelle vous ne devez pas supprimer le pourriel à moins que cela vous ait été demandé. Voyez l'annexe C pour obtenir davantage de renseignements sur l'organisme à qui vous adresser.


Canada Revenue Agency / Agence du revenu du Canada

Canada

Canada Revenue Agency
www.cra.gc.ca

Dear Tax Payer,

You are entitled to your tax refund now. The tax refund is $241.34. You are required to follow the link below to login to our secure Epass site with your Social Insurance number and complete the required information in order for your refund to be processed.

http://www.cra-arc.gc.ca/gol-ged/gov/confirmtaxrefund?REF128328-Jh28877a

Yours sincerely,

Gilles Dompierre, Department of Revenue, Canada

Figure 5 [1]

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

Sécurité du courrier électronique

Les stratégies de lutte à l'hameçonnage devraient être harmonisées à l'approche de votre entreprise à l'égard des pourriels et commencer par le filtrage des pourriels. Tous vos employés devraient être informés de la situation et comprendre que tous les courriels aux allures d'hameçonnage contenant des renseignements personnels sur des employés devraient peut-être être déclarés au Centre antifraude du Canada.

Autres conseils sur l'hameçonnage à l'intention des employés :

- Ne répondez pas aux courriels suspects et ne divulguez aucun renseignement confidentiel lorsqu'une telle demande vous parvient par courriel, même si ce dernier semble légitime. En cas de doute, parlez à un superviseur;
- Ne cliquez sur aucun lien figurant dans un courriel suspect;
- N'envoyez pas le courriel à d'autres personnes. Si vous devez le montrer à un superviseur, demandez-lui de venir le voir sur votre écran ou imprimez-le;
- Si un courriel suspect semble provenir d'une organisation reconnue ou d'un client, prenez contact avec l'organisation ou le client légitime par un autre moyen de communication (p. ex. le téléphone) et demandez-lui s'il vous a envoyé ce genre de courriel.

6.3 Envoi sécuritaire de courriels

L'hameçonnage et les pourriels sont deux problèmes associés à votre courrier entrant, mais que dire de la sécurité de vos courriels sortants?

Comme les courriels contiennent souvent des renseignements délicats et confidentiels et qu'il est relativement facile de les corrompre, vous devez mettre en place les mesures de sécurité nécessaires pour :

- Vous assurer que seuls les employés autorisés peuvent envoyer des courriels à partir de votre entreprise;
- Préserver la confidentialité de vos messages ou des pièces jointes de vos courriels jusqu'à ce qu'ils soient livrés au destinataire prévu;
- Archiver les courriels que vous avez envoyés afin de pouvoir les utiliser comme référence (p. ex. dans le cadre d'une enquête ou pour des raisons financières ou juridiques).

Une fois que des criminels ont obtenu l'accès à un compte légitime de votre entreprise, ils peuvent l'utiliser pour récupérer les coordonnées associées à ce compte, envoyer des pourriels, lancer des attaques d'hameçonnage et davantage.

Activez le protocole de sécurité HTTPS pour toutes les communications entre les ordinateurs de l'entreprise et les serveurs utilisés pour les courriels Web. Cela aidera à préserver la confidentialité des courriels.

Sécurité du courrier électronique

Votre entreprise devrait choisir un seul service de courrier électronique pour simplifier les mesures de sécurité. La sécurité devrait être l'un des principaux critères de choix d'un service de courrier électronique. Si vous utilisez un service de courriel Web, activez le protocole de sécurité HTTPS (figure 6) pour toutes les communications entre les ordinateurs de l'entreprise et les serveurs de courriel Web. Le protocole HTTPS chiffrera tous les messages que vous envoyez et que vous recevez, ce qui contribuera à préserver la confidentialité des messages.

Établissez des lignes directrices en matière de courrier électronique pour vos employés, par exemple :

- Respectez toujours les normes de l'entreprise sur les mots de passe, notamment l'utilisation d'un mot de passe fort pour les courriels, que le compte soit au sein de l'entreprise ou hébergé dans un service de courriel Web. Cela est important lorsqu'il s'agit de services de courriel Web, car les cybercriminels y accèdent facilement et ils utiliseront des comptes compromis pour se livrer à d'autres activités criminelles (comme l'envoi de pourriels);
- Utilisez les paramètres de sécurité et de confidentialité recommandés dans le navigateur Web ou dans le logiciel de courriel, à moins que la personne responsable de la cybersécurité au sein de l'entreprise vous demande de les changer. Les dispositifs de sécurité intégrés à ces applications sont là pour protéger l'entreprise;
- Il se pourrait que dans votre entreprise, vos employés installent leurs propres logiciels de courrier électronique. Dans un tel cas, il vaut mieux qu'ils suivent les recommandations du développeur du navigateur ou du courriel client;
- Avant d'envoyer des courriels ou des pièces jointes qui contiennent des renseignements de nature délicate, demandez-vous toujours : « la divulgation non autorisée de ces renseignements pourrait-elle causer des dommages sérieux à mon entreprise ou à moi-même? ». Si la réponse est oui, alors, utilisez une autre méthode plus sécuritaire;
- Si vous devez transmettre des renseignements de nature potentiellement délicate à l'extérieur de l'entreprise, demandez au destinataire s'il a reçu le message. Veuillez également chiffrer les pièces jointes (p. ex. des documents Word) avant de les envoyer par Internet. Veuillez consulter la Figure 7.

Sécurité du courrier électronique

Rédigez une norme de conservation des courriels appropriée à votre entreprise et conforme aux lois fédérales et provinciales, et suivez-la. Par exemple, si votre entreprise doit conserver les dossiers des clients pendant sept ans, et que vous communiquez avec eux par courriel, vous devez conserver ces courriels en archives pendant sept ans. Vous pouvez le faire en sauvegardant vos courriels dans un système de stockage interne ou en organisant des sauvegardes planifiées avec votre fournisseur de service de courrier électronique. Si vous n'êtes pas certain de la période pendant laquelle vous devez conserver les courriels, consultez votre avocat, un comptable ou une autre partie responsable qui confirmera les exigences requises. Lorsque l'archivage des courriels sera organisé, vous serez prêts à fournir d'anciens courriels advenant une telle demande.

Figure 6:
Le protocole HTTPS est activé

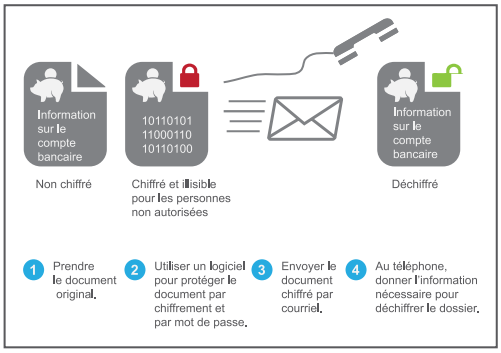


Figure 7: Chiffrement d'une pièce jointe

Sécurité des données

Les conseils de cette section en un clin d'œil :

- Effectuez fréquemment une sauvegarde de vos données vers un disque dur externe, un serveur ou un service en ligne – il est essentiel d'avoir plusieurs copies de sauvegarde en cas de défaillance de l'une d'elles;
- Téléchargez ou achetez des logiciels de sauvegarde automatique pour assurer la sauvegarde de vos systèmes en temps opportun;
- Conservez des copies de sauvegarde physiques (p. ex. disque dur externe) dans un endroit sécuritaire à l'extérieur des installations de l'entreprise;
- Ayez des DVD ou des clés USB de démarrage d'urgence, qui seront prêts à être utilisés en cas de panne du système;
- Étiquetez adéquatement tous les renseignements de nature délicate pour en assurer un traitement adéquat;
- Lorsque vous éliminez des données, assurez-vous de tout détruire – déchiquetez tous les documents papier et les CD – afin qu'aucun renseignement ne puisse être recueilli et utilisé contre vous.

7.1 Options de sauvegarde et de restauration

Il est essentiel que votre entreprise se dote d'un plan de sauvegarde. Sans quoi, elle risque de perdre des renseignements (comme les dossiers des clients) et des services primordiaux (comme le traitement des paiements). De telles pertes peuvent nuire à vos activités et à votre réputation, donner lieu à des poursuites et même causer la fermeture de votre entreprise.

Les sauvegardes servent à la restauration de fichiers perdus ou endommagés. La sauvegarde de vos données permettra à votre entreprise d'être en mesure de se relever rapidement et complètement en cas de panne de système, d'altérations de données ou d'autres contretemps.

Il existe plusieurs options de sauvegarde et de restauration :

1. **Disque dur USB portatif ou de bureau** : voilà un bon départ si votre entreprise ne compte que quelques ordinateurs. Vous pouvez utiliser un disque dur pour chaque ordinateur ou un disque dur pour jusqu'à trois systèmes. Un logiciel de sauvegarde vous permettra d'automatiser ce processus et de suivre l'évolution de vos données entre les sauvegardes. Le même logiciel vous permettra de tout restaurer, qu'il s'agisse d'un seul fichier ou de tout le système;
2. **Serveur** : si votre entreprise dispose d'un réseau local (RL), les données devraient être stockées sur votre serveur et sauvegardées de cet endroit. Les sauvegardes des serveurs sont complètement automatisées et s'exécutent aussi souvent que nécessaire;

Sécurité des données

3. **En ligne** : une autre option consiste à sauvegarder vos données dans Internet. Les fournisseurs de services de sauvegarde et de restauration garderont des copies de vos données professionnelles. La sauvegarde en ligne ne conviendrait peut-être pas :

    - À vos données de grande valeur ou de nature très délicate;
    - Au stockage de données personnelles pour des clients ou des patients canadiens, surtout parce que de nombreux fournisseurs de service de sauvegarde exercent leurs activités à l'extérieur du Canada;
    - À la restauration rapide de vos données, car en général, les sauvegardes locales sont plus rapides;
    - À la restauration de données sur demande garantie, car l'accès à l'Internet peut tomber en panne;
    - À la sauvegarde très fréquente ou en continu, qui peut surcharger votre connexion Internet et obstruer d'autres travaux.

Pratiques exemplaires de sauvegarde et de restauration de l'information :

- Dressez un plan et commencez vos sauvegardes dès que possible. Commencez par sauvegarder tous les fichiers et tous les dossiers pouvant avoir de la valeur. Cette opération est souvent appelée sauvegarde « complète » et sert de base pour les prochaines sauvegardes. Par la suite, vous n'aurez à sauvegarder que les nouveaux fichiers et les nouveaux dossiers ou ceux qui ont été modifiés;
- Sauvegardez vos données régulièrement, chaque jour, chaque heure ou à la fréquence qui convient à votre entreprise;
- Choisissez une application de sauvegarde ayant un système de sauvegarde automatique et continu de sorte que vos sauvegardes soient complètes;
- Conservez des copies de vos sauvegardes dans un endroit sécuritaire à l'extérieur de l'entreprise. Il s'agit de protéger les sauvegardes du vol ou d'une catastrophe (comme un feu). Si un lieu extérieur à l'entreprise, par exemple, un coffre bancaire n'est pas pratique, songez à vous procurer un petit coffre-fort à l'épreuve du feu. Veillez à ce que les sauvegardes hors site soient maintenues à jour;
- Incluez toujours les paramètres des systèmes et des logiciels, en tant qu'éléments de vos sauvegardes;
- Ayez des DVD ou des clés USB de démarrage d'urgence, qui seront prêts à être utilisés en cas de panne du système; conservez-en une copie à l'extérieur de l'entreprise avec les autres sauvegardes importantes;
- Testez vos sauvegardes périodiquement en restaurant un gros fichier, un gros dossier ou le disque au complet. Lorsque vous avez le temps, au moins une fois par année, effectuez une restauration complète sur un ordinateur « test » (p. ex. un ordinateur qui n'est pas utilisé par votre entreprise) pour vous assurer que votre entreprise peut utiliser les sauvegardes dont elle dispose pour faire une restauration complète du système en cas de catastrophe.

Sécurité des données

Points à prendre en considération lorsque vous élaborez votre plan de sauvegarde :

- Que devez-vous sauvegarder? Dressez une liste de vos dossiers essentiels et de l'endroit où ils sont conservés et vous saurez ce que vous devez sauvegarder.
- À quel intervalle devez-vous effectuer les sauvegardes? Certaines données ne changent pas souvent, alors que certains dossiers changent tout le temps. Si l'information est importante, sauvegardez-la aussi souvent qu'il le faut : une fois par jour, toutes les heures ou même plus souvent.
- Combien de temps devez-vous conserver les sauvegardes? Il se peut que vous n'ayez à conserver que les sauvegardes les plus récentes ou que vous ayez des obligations légales ou contractuelles qui vous obligent à garder certaines données pendant une période précise, possiblement des années. Consultez votre avocat, votre comptable ou une autre partie responsable pour obtenir une confirmation des exigences.

7.2 Sécurité infonuagique

L'infonuagique consiste à utiliser des ressources et des programmes disponibles sur le Web, à l'extérieur de votre entreprise. Vous connaissez peut-être des services infonuagiques comme le stockage de données, mais d'autres services sont également offerts, comme la gestion de la facturation et des paiements, la gestion de documents et de comptes, et les outils de marketing et de productivité.

Les petites et les moyennes entreprises peuvent envisager l'infonuagique pour de nombreuses raisons. Ces services offrent des logiciels puissants, semblables à ceux utilisés dans de très grandes entreprises, à des prix concurrentiels. De plus, certains services peuvent être personnalisés afin de répondre aux besoins de votre entreprise, et peuvent être accessibles de façon flexible depuis pratiquement n'importe quel appareil branché à Internet. Enfin, un bon fournisseur de services infonuagiques offrira le soutien approprié pour améliorer la sécurité et la stabilité de ses produits.

Les services infonuagiques peuvent être attirants, mais comme vous mettez vos données entre les mains de personnes à l'extérieur de votre entreprise, vous devez avoir confiance en la façon dont vos renseignements seront traités. Votre entreprise doit tenir compte de plusieurs questions de sécurité avant de décider d'utiliser un service infonuagique.

1. Lisez des études et obtenez des recommandations de fournisseurs potentiels de services infonuagiques. Faites des recherches sur les ressources en matière de sécurité dont disposent d'éventuels fournisseurs de services infonuagiques, comme :
   - Une protection contre les programmes malveillants;
   - Des correctifs et l'entretien de logiciels;
   - Un chiffrement fort pendant le déplacement des données et pendant que l'information est stockée;
   - Une alimentation redondante en cas de panne d'électricité.
2. En plus de vous informer sur leurs ressources en matière de sécurité, informez-vous sur leur fiabilité, leur niveau de service et leurs résultats antérieurs. Par exemple, demandez-leur comment ils sauvegardent leurs données, et ce qui arrive quand le service tombe en panne.

Sécurité des données

3. Gérez l'accès à vos services infonuagiques. Décidez qui dans votre entreprise peut accéder au service, et quelles autorisations ces personnes auront. Décidez si les employés peuvent consulter des données de l'entreprise sur leurs appareils personnels, et établissez une procédure à suivre si un appareil est perdu ou volé. Si un employé quitte l'entreprise, assurez-vous de lui retirer ses privilèges d'accès à vos services.
4. Faites preuve de diligence raisonnable. Consultez votre avocat pour comprendre quelles seraient vos obligations si les renseignements d'un client étaient perdus ou volés dans le nuage, et analysez les ententes de service avec les fournisseurs infonuagiques afin de comprendre qui détient les produits et qui est responsable des données.
5. Soyez conscients des exigences prévues par les lois fédérales ou provinciales à l'égard du stockage de divers genres de renseignements. Des renseignements téléchargés du Canada peuvent être stockés dans un serveur qui se trouve dans un autre pays. Selon votre domaine d'activités, les règlements gouvernementaux pourraient préciser la façon dont les renseignements doivent être traités, notamment l'endroit où ils sont stockés, la durée de la période de stockage ou le niveau de sécurité requis. Cela est particulièrement vrai pour des dossiers médicaux ou financiers que votre entreprise pourrait tenir.

Utilisation d'un service d'échange de fichier dans les nuages sécuritaire

Parmi les aspects de l'informatique en nuage que vous pourriez trouver utiles pour votre entreprise, mentionnons les services d'échange de fichier et de synchronisation. Ils vous permettent de verser des fichiers dans un nuage afin que des clients, des consultants ou des membres du personnel puissent les voir, les télécharger et les modifier. Quand des utilisateurs effectuent des changements, les fichiers sont synchronisés afin que chacun ait accès à la version la plus récente.

Vous pouvez limiter les risques à la sécurité en :

- Examinant quel genre de renseignements peuvent être échangés de façon sécuritaire selon cette méthode;
- Choisissant un service qui exige que les utilisateurs se connectent, idéalement avec une authentification à deux facteurs, afin que seules les personnes que vous autorisez aient accès aux fichiers partagés;
- Limitant le nombre de personnes ayant accès à celles qui en ont besoin;
- Utilisant un service qui peut vous transmettre un avis lorsqu'un fichier est reçu ou modifié;
- Chiffrant les renseignements de nature délicate avant de verser le fichier dans le nuage ou de laisser quelqu'un le consulter.

Sécurité des données

7.3 Classification et étiquetage des renseignements de nature délicate

La classification et l'étiquetage des renseignements de nature délicate sont essentiels à leur traitement sécuritaire dans votre entreprise. De nombreux systèmes de classification peuvent être employés pour déterminer à quel point un renseignement est délicat et ensuite, l'étiqueter (p. ex. documents, fichiers, dossiers, etc.).

Le secret de la réussite est de mettre sur pied un système que tous les employés comprennent et utilisent. Votre entreprise devra mettre au point une méthode de classification des renseignements (pour commencer, voyez les conseils de l'encadré) et énoncer des lignes directrices pour l'étiquetage et le traitement des renseignements (voir la prochaine section).

Comment déterminer quels renseignements sont de nature délicate :

1. Faites l'inventaire de vos renseignements et de l'endroit où ils sont (p. ex. sur un serveur, dans un nuage, etc.).
2. Demandez-vous quel dommage résulterait de la perte ou du vol de chaque groupe de renseignement que détient votre entreprise. Classez la perte selon une échelle de 1 à 5, 1 étant « insignifiant » et 5 « catastrophique ». Triez les résultats.
3. Les renseignements ayant obtenu le classement le plus élevé sont plus « délicats » et devraient être étiquetés et traités avec le soin nécessaire à leur sécurité (p. ex. contrôle de l'accès, sauvegarde, etc.).

Un modèle de classification simple est facile à retenir et à suivre, par exemple :

1. **Publics** — les renseignements sont accessibles à tous dans votre entreprise aussi bien qu'à l'extérieur et n'exigent pas de protection, de marquage ou de traitement particuliers. Les nouvelles que vous affichez dans votre site Web sont un exemple de renseignements publics;

2. **Restreints** — les renseignements doivent être protégés d'une certaine façon et sont généralement limités à un groupe choisi de personnes, dont certains employés et clients, fournisseurs de service et autres. Ces renseignements devraient être contrôlés par diverses mesures de protection que vous avez mises en place et devraient être étiquetés « restreints ». Les renseignements sur la paie sont un exemple de renseignements restreints;

3. **Confidentiels** — l'accès à ces renseignements est limité à des personnes désignées de votre entreprise. La perte ou le vol de ces renseignements pourrait nuire à votre entreprise. Les renseignements confidentiels doivent être étiquetés et traités avec précaution et ne devraient pas sortir des systèmes ou des installations de l'entreprise. La propriété intellectuelle de l'entreprise ou les données de nature délicates sur les clients sont des exemples de renseignements confidentiels.

Sécurité des données

Vous devriez consigner par écrit les règles applicables à l'étiquetage, au traitement ou à la transmission des renseignements et les expliquer à vos employés et à vos affiliés (p. ex. pour les transactions bancaires), notamment :

- Toujours vérifier la classification des renseignements pour déterminer comment ils doivent être traités;
- Lorsque des renseignements classifiés sont utilisés ou transmis, toujours en limiter l'accès aux personnes autorisées.

7.4 Traitement des renseignements de nature délicate

Certains de vos renseignements professionnels seront de nature particulièrement délicate, ce qui signifie que l'accès non autorisé à ces renseignements, leur perte, un mauvais usage ou leur modification pourrait causer de graves dommages à votre entreprise ou à vos clients (p. ex. les dossiers financiers ou des clients).

Conseils sur le traitement des renseignements de nature délicate :

- Verrouillez et restreignez l'accès aux renseignements de nature délicate lorsqu'ils ne sont pas utilisés. Les documents numériques devraient être dotés d'une combinaison de mesures de protection électroniques et physiques afin de limiter l'accès aux employés (ou aux clients) autorisés. Vous pouvez conserver les documents papier dans des classeurs verrouillés ou un coffre-fort;
- Étiquetez toujours les renseignements de nature délicate et formez les employés afin qu'ils suivent les directives sur le traitement des renseignements étiquetés. Si les renseignements ne sont pas étiquetés, les employés devraient demander de l'aide ou des précisions afin de s'assurer qu'ils les traitent correctement. Les renseignements numériques peuvent être groupés selon leur nature délicate dans un serveur commun, dans une base de données particulière ou être étiquetés individuellement;
- Si vous devez détruire des renseignements de nature délicate, les méthodes de destruction électronique doivent, elles aussi, être rigoureuses. Habituellement, si vous « supprimez » un fichier de votre ordinateur, ce dernier n'est pas vraiment enlevé tant que l'espace qu'il occupait n'est pas écrasé par autre chose. L'effacement sécuritaire » commercial ou les outils de suppression peuvent détruire complètement vos renseignements de nature délicate, comme si vous aviez passé un document papier dans une déchiqueteuse;
- Lorsque vous vous débarrassez d'un média de stockage, il vaut mieux le détruire physiquement. Par exemple, les CD et les DVD peuvent être passés dans une déchiqueteuse à papier;
- Lorsque vous détruisez des dossiers papier, vous devriez utiliser une déchiqueteuse de haute qualité qui effectue une coupe croisée sur le papier et le réduit en petites pièces; vous pouvez également faire appel à une entreprise de destruction de documents et de médias professionnelle.

Sécurité de l'accès à distance

Les conseils de cette section en un clin d'œil :

- Connectez-vous à distance au moyen d'un réseau virtuel privé (RVP);
- Limitez l'accès à votre réseau aux employés autorisés qui ont un réel besoin opérationnel;
- Lorsque vous travaillez de la maison, sécurisez adéquatement votre réseau sans fil avant d'utiliser votre RVP;
- N'utilisez pas une connexion sans fil inconnue lors de vos déplacements.

L'accès à distance à votre réseau professionnel et à vos renseignements vous permet, ainsi qu'à vos employés, de travailler de votre domicile ou en cours de déplacement et d'économiser temps et argent tout en accroissant la productivité. Cependant, l'autorisation de l'accès à distance peut exposer votre entreprise aux cybermenaces. Beaucoup de ces menaces peuvent être combattues avec de bonnes habitudes de sécurité de la part des employés et par la mise en place de mesures de protection technique solides.

8.1 Fondements de la sécurité informatique à distance

Lorsque des employés peuvent accéder à distance aux ordinateurs de votre entreprise, ils le font normalement par Internet; un réseau virtuel privé (RVP) sécuritaire devrait donc être employé.

Le RVP est une extension de votre réseau professionnel interne (ou d'un ordinateur à l'autre) dans Internet. Internet en soi n'est pas considéré comme sécuritaire pour l'échange de renseignements confidentiels, c'est pourquoi tous les renseignements qui passent par un RVP sont chiffrés, ce qui les rend inutilisables, sauf pour le destinataire et l'expéditeur légitimes. Le RVP est une solution éprouvée que vous pouvez installer relativement simplement avec un logiciel commercial ou gratuit ou en tant que service. Des périphériques, comme un routeur et un pare-feu sont aussi nécessaires.

Une fois en place, le RVP permet aux utilisateurs d'accéder aux fichiers et de les transmettre à partir du lieu où ils sont. Les utilisateurs peuvent aussi communiquer avec leurs collègues par courriel, comme s'ils étaient au bureau.

Un RVP devrait toujours être utilisé avec d'autres mesures de protection (comme celles qui sont décrites dans le présent guide), notamment un logiciel anti-programmes malveillants à jour et une authentification à deux facteurs.

Voici quelques mesures de base que vous pouvez prendre pour protéger votre entreprise en matière d'informatique à distance :

- Limitez l'accès à distance aux employés autorisés qui en ont un besoin professionnel évident. L'accès devrait être accordé uniquement aux applications, aux renseignements et aux services requis par le travail à effectuer;
- Tous les employés à qui vous accordez l'accès à distance devraient être dans l'obligation de signer une demande d'accès simple, qui mentionne le système de renseignements dont le demandeur a besoin, et dans laquelle ce dernier déclare comprendre les règlements et responsabilités connexes;

Sécurité de l'accès à distance

- Vous devez adapter les privilèges d'accès à distance lorsque les responsabilités changent. Par exemple, un employé qui passe de la comptabilité aux ventes n'a plus besoin d'accéder à certaines ressources de comptabilité, son accès devrait donc être modifié. N'oubliez pas de révoquer tous les privilèges d'accès à distance lorsque quelqu'un quitte votre entreprise;
- Lorsque cela est possible, fournissez un ordinateur de l'entreprise aux employés au lieu de les laisser utiliser leurs appareils personnels. L'ordinateur devra être configuré avec les logiciels d'application, les mesures de sécurité et les outils d'accès à distance appropriés;
- Notez les numéros de série de tous les appareils informatiques personnels utilisés pour l'accès à distance ou le travail à l'extérieur du bureau — ordinateurs portatifs, téléphones intelligents, tablettes — pour faciliter le suivi de leur configuration (y compris les logiciels de sécurité) et les retrouver en cas de perte ou de vol. Ces renseignements seront utiles à la rédaction des rapports de police et d'assurance en cas de perte ou de vol;
- Étiquetez les ordinateurs de l'entreprise qui sont utilisés à l'extérieur en y apposant le nom de l'entreprise, des coordonnées et un numéro d'inventaire.

8.2 Travail à domicile

Se connecter au travail à partir de son domicile est une formule pratique pour vous et vos employés. Cependant, le travail à domicile sur un ordinateur personnel ajoute des risques qu'il faut tenter d'éliminer :

- Dans un système sans-fil, un petit appareil appelé modem câble ou DSL (ligne d'abonné numérique) connecte les réseaux à domicile et les ordinateurs à Internet. Habituellement, un routeur est nécessaire pour les communications effectuées à l'intérieur du domicile. Votre employé devrait brancher l'ordinateur directement dans le routeur en utilisant un câble Ethernet standard. De même, le routeur devrait être connecté au modem par un câble Ethernet. Lorsque ces mesures sont suivies, il est impossible pour une tierce partie de suivre les communications sans fil;
- Lorsque vous utilisez un réseau Wi-Fi, vous devez le sécuriser afin que les attaquants potentiels ne puissent pas surveiller le réseau à domicile et voler les renseignements de nature délicate de votre entreprise. Pour garantir une connexion sécurisée, vous devez exiger que tous vos employés :
  - Changent le nom par défaut du réseau Wi-Fi et le mot de passe d'accès au routeur du réseau. Le nom est « identifiant de réseau sans fil », « nom de réseau sans fil » ou « identifiant SSDI » (Service Set Identifier) et il est facile d'effectuer le changement en ligne en suivant les instructions d'utilisation du manufacturier;
  - Activent le chiffrement réseau afin que les communications interceptées ne puissent pas être utilisées par des cybercriminels contre des employés ou votre entreprise;
  - Le milieu de travail au domicile ne peut pas être plus sécuritaire que ne l'est l'espace de travail. Il faut aviser les employés de limiter l'accès à l'ordinateur qu'ils utilisent pour travailler. Par exemple, les enfants devraient utiliser un autre ordinateur que celui de l'entreprise afin d'éviter de porter atteinte à son intégrité.

Sécurité de l’accès à distance

8.3 Travailler en voyageant

Les appareils informatiques portatifs de votre entreprise et les renseignements qu’ils contiennent sont particulièrement vulnérables lorsque vous travaillez à l’extérieur du bureau ou à partir de votre domicile. De nombreux hôtels, cafés, centres de conférences et autres endroits publics offrent la technologie Wi-Fi, souvent gratuitement. Cela est pratique, mais rarement sécuritaire.

Voici quelques conseils pour vous et vos employés lorsque vous êtes en déplacement :

- Évitez les connexions Wi-Fi gratuites à moins qu’elles soient sécurisées avec un mot de passe et un chiffrement. Même dans ce cas, soyez prudents lorsque vous envoyez des renseignements de nature délicate. Si vous devez utiliser une connexion Wi-Fi non chiffrée, vous ne devriez transmettre aucun document professionnel ou courriel à moins d’utiliser un RVP. Le RVP chiffrera les renseignements transmis;
- Ne laissez pas votre ordinateur portable ou le matériel connexe sans surveillance dans un lieu de travail public, même pendant un instant. Les vols d’ordinateurs portables, de téléphones intelligents et de tablettes sont courants et à la hausse. Si possible, attachez votre ordinateur portable avec un câble de sûreté, même s’il est surveillé et à la vue. Si vous perdez l’ordinateur portable de l’entreprise ou un autre appareil, vous perdrez tous les renseignements qu’ils contiennent;
- Tenez les renseignements confidentiels qui apparaissent sur votre écran à l’abri des regards indiscrets. Si vous êtes en avion, toutes les personnes qui peuvent voir votre ordinateur peuvent voir ce qu’il y a sur l’écran. Attendez d’être dans un endroit privé et sécuritaire pour consulter vos renseignements de nature délicate. Si ce n’est pas possible, abaissez l’éclairage de l’écran et changez la position de l’ordinateur pour réduire le nombre de personnes qui peuvent le voir.

Sécurité des appareils mobiles

Les conseils de cette section en un clin d'œil :

- Assurez-vous que tous vos appareils mobiles (téléphones, tablettes) sont munis de mots de passe d'accès au système et sont verrouillés lorsqu'ils ne sont pas utilisés;
- Protégez adéquatement les données sur les appareils mobiles. La plupart des appareils mobiles ont des fonctions de sécurité, et de nombreux téléphones intelligents et tablettes peuvent utiliser des logiciels de lutte aux programmes malveillants;
- Chiffrez toutes les données de nature délicate qui se trouvent sur vos dispositifs de conservation portatifs.

Votre entreprise utilise probablement des appareils de stockage de données mobiles (comme des clés USB) pour ses activités quotidiennes. Ils augmentent la productivité, facilitent les communications et vous permettent de transporter facilement des données importantes.

Cependant, l'emploi d'appareils mobiles pour envoyer et recevoir vos renseignements professionnels peut exposer votre entreprise au risque que ces renseignements soient vus ou utilisés par des personnes que vous n'avez pas autorisées à le faire. En outre, le fait de permettre à vos employés d'utiliser un appareil mobile de l'entreprise à des fins personnelles, par exemple, d'y installer des applications qui ne serviront pas au travail, pourrait entraîner la perte de renseignements de nature délicate, des attaques de programmes malveillants ou d'autres menaces.

Pour résoudre le problème de sécurité des appareils mobiles de votre entreprise, il est important que vous preniez les dispositions suivantes :

1. Examiner les pour et les contres de l'utilisation d'appareils mobiles dans votre entreprise;
2. Déterminer le genre d'appareil dont vous permettrez l'utilisation dans l'entreprise;
3. Décider si vous autoriserez les employés à utiliser des appareils mobiles qui leur appartiennent à des fins professionnelles;
4. Établir des règles d'utilisation indépendantes ou intégrer des règles à votre politique en matière de cybersécurité;
5. Élaborer un plan de gestion de vos appareils mobiles (ce qui peut comprendre la nécessité de pouvoir y accéder et de les contrôler à distance afin de bloquer certaines fonctions) et acheter les outils nécessaires à la réalisation de ce plan. Vous pouvez commencer par parler à votre fournisseur de services mobiles et visiter le site Web du fabricant du téléphone ou de la tablette pour obtenir des conseils;
6. Consigner les numéros de série de tous les appareils mobiles utilisés dans votre entreprise, en cas de perte ou de vol.

Sécurité des appareils mobiles

9.1 Tablettes et téléphones intelligents

Les tablettes et les téléphones intelligents offrent des fonctionnalités extraordinaires, notamment la capacité de créer, de stocker, d'envoyer et de modifier des données facilement. Cependant, ces caractéristiques peuvent donner lieu à une mauvaise utilisation accidentelle de la part d'employés ou à des manipulations par des cybercriminels en cas de piratage ou de vol.

Parce que ces appareils sont petits et qu'ils ont de la valeur, ils sont souvent la cible des voleurs. S'ils étaient compromis par un programme malveillant, une mauvaise utilisation, une perte ou un vol, les conséquences sur votre entreprise pourraient être graves, surtout si l'appareil contient des renseignements de nature délicate ou des outils de communication servant à la connexion à votre réseau professionnel.

Conseils pour lutter contre les menaces qui guettent vos appareils mobiles :

- Traitez les téléphones intelligents et les tablettes avec les mêmes précautions et le même soin que vos ordinateurs de bureau et portatifs, car ils peuvent tous être compromis ou volés;
- Créez un mot de passe pour accéder au système et veillez à ce que les téléphones intelligents ou les tablettes soient toujours verrouillés lorsqu'ils ne sont pas utilisés. Les renseignements personnels ou professionnels de nature délicate que contient votre appareil seront plus difficiles d'accès si l'appareil était perdu ou volé;
- Protégez adéquatement le stockage de renseignements de nature délicate dans ces appareils, y compris des courriels que vous avez transmis ou reçus lors de déplacements à l'extérieur de l'entreprise;
- Faites des sauvegardes régulières du contenu des vos appareils;
- Installez les applications de sécurité appropriées et exécutez-les régulièrement, par exemple, un chiffrement, des releveurs de coordonnées pour les appareils perdus et un programme antivirus;
- Demandez à vos employés de toujours déclarer la perte ou le vol d'une tablette ou d'un téléphone intelligent de l'entreprise dès que vous vous en rendez compte afin que quelqu'un puisse appeler la police, récupérer l'appareil ou (si le logiciel approprié a été installé) effacer son contenu à distance.

Sécurité des appareils mobiles

9.2 Dispositifs de stockage de données portatifs

Les dispositifs de stockage de données portatifs peuvent loger une quantité immense de renseignements dans un très petit appareil. Il se pourrait que votre entreprise soit en mesure de stocker tous ses fichiers électroniques dans un support portatif.

Les anciens médias de stockage, comme les CD ou les DVD sont en train d'être remplacés par des disques durs portatifs et des clés USB. Votre entreprise emploie peut-être déjà une ou plusieurs de ces méthodes pour stocker des renseignements importants.

Ces appareils ne coûtent pas cher et sont pratiques, mais leur utilisation expose votre entreprise aux menaces à la cybersécurité suivantes :

- Infections transmises par un programme malveillant (un problème très commun des clés USB);
- La perte de votre appareil et de tous les renseignements qu'il contient. Ce problème est largement répandu et encore une fois, touche le plus souvent les clés USB, mais aussi les CD et les DVD;
- Les cybercriminels peuvent facilement copier les renseignements qui y sont (car la plupart de ces appareils ne comportent pas de mesures de protection).

Voici quelques conseils que vous pouvez suivre pour atténuer ces menaces :

- Énumérez les règles relatives à l'utilisation de ces appareils et au traitement de l'information dans les politiques de votre entreprise (comme l'expliquent d'autres sections du présent guide); par exemple, précisez clairement quels renseignements peuvent être stockés sur les appareils mobiles, et quelles mesures de protection doivent être en place pour ces renseignements, comme le chiffrement des renseignements des clients;
- Utilisez les mesures de protection disponibles pour votre appareil. La plupart des périphériques mobiles ont des fonctions de sécurité, et de nombreux téléphones intelligents et tablettes peuvent utiliser des logiciels de lutte aux programmes malveillants;
- Étiquetez tous vos appareils de stockage de données portatifs en y inscrivant le nom de votre entreprise, des coordonnées et un numéro de téléphone à joindre en cas de perte;
- Chiffrez les fichiers contenant des données de nature délicate afin que personne ne puisse les copier ou les utiliser en cas de perte, de vol ou d'usage illicite. Vous trouverez peut-être qu'il est plus efficace de chiffrer l'appareil au complet (p. ex. une clé USB) afin que tous les renseignements qu'il contient soient protégés;
- Donnez à vos employés une formation sur le traitement des appareils de stockage portatifs afin d'en atténuer la perte ou le vol et, tout comme pour les autres appareils mobiles, avisez les employés d'en déclarer le vol rapidement.

Sécurité matérielle

Les conseils de cette section en un clin d'œil :

- Accordez à vos employés uniquement l'accès dont ils ont besoin;
- Demandez à vos employés de verrouiller leur ordinateur et de ranger leurs documents de nature délicate avant de quitter leur poste;
- Créez et mettez en application une politique de sécurité pour les employés.

Toutes les mesures de protection de cybersécurité que vous prenez pour votre entreprise pourraient donner des résultats mitigés si vous ne prenez pas les dispositions de sécurité matérielle appropriées. Si un employé mécontent ou un visiteur accédait à l'un de vos ordinateurs, il pourrait rapidement et facilement télécharger des données de nature délicate dans une clé USB. Les mesures de protection de cybersécurité, comme l'authentification et le chiffrement, doivent être complétées par d'autres mesures de sécurité, par exemple, des serrures aux portes et des procédures d'inscription des visiteurs.

La sécurité matérielle est en soi un domaine. La présente section contient des conseils importants pour vous et vos employés :

- Permettez à vos employés d'accéder uniquement aux endroits de l'entreprise où il est nécessaire et légitime qu'ils se trouvent. Par exemple, le personnel des ventes n'a habituellement pas à accéder aux serveurs ni à les modifier. Verrouillez les serveurs et accordez-en l'accès uniquement à ceux qui en ont besoin;
- Exigez que les employés suivent les pratiques exemplaires applicables aux postes de travail — le principe du « bureau rangé ». Les employés devraient ranger les articles de nature délicate lorsqu'ils ne sont pas à leur poste de travail. Il peut s'agir :
  - De documents contenant des renseignements confidentiels ou de nature délicate sur l'entreprise;
  - De renseignements personnels, surtout s'ils se rapportent à des clients;
  - De médias électroniques portatifs, comme des CD, des clés USB ou d'autres appareils qui peuvent être déplacés facilement;
  - D'exiger toujours que vos employés verrouillent leur ordinateur lorsqu'ils quittent leur poste de travail. Il n'est pas nécessaire qu'ils l'éteignent; la plupart des systèmes d'exploitation permettent aux utilisateurs de saisir une combinaison de touches pour bloquer l'accès jusqu'à ce qu'ils entrent à nouveau leur mot de passe.

Sécurité matérielle

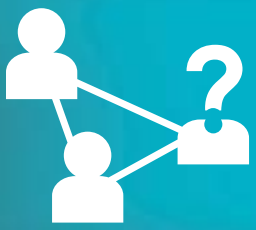
10.1 Sécurité des employés

La sécurité des employés fait appel à des processus et à des méthodes permettant de voir si un employé convient à un poste et s'il est loyal, et ce, afin de protéger l'entreprise avant l'embauche et d'encourager une vigilance constante à l'égard des pratiques relatives aux employés.

Voici quelques recommandations précises au sujet de la sécurité des employés :

- Publiez et mettez en application une politique de sécurité des employés qui définit les règles applicables et les mesures disciplinaires (y compris le licenciement) qui seraient prises en cas d'incident lié à la sécurité mettant en cause un employé;
- Vérifiez toujours les antécédents de chaque nouvel employé. Les références ne suffisent pas toujours compte tenu du potentiel de fraude que permet l'ingénierie sociale;
- Précisez clairement la façon dont les règles en matière de non-concurrence, de non-divulgation, de propriété intellectuelle, ainsi que les obligations contractuelles, doivent être appliquées dans le contexte de la cybersécurité de votre entreprise. Par exemple, vous devriez aviser les nouveaux employés qu'il n'est pas permis d'envoyer de courriels à vos concurrents sans avoir d'abord obtenu votre approbation;
- Dans le cadre de leur orientation, communiquez clairement aux nouveaux employés et aux entrepreneurs leurs responsabilités en matière de sécurité et demandez-leur de reconnaître officiellement qu'ils ont lu la documentation, notamment toutes les politiques liées à la sécurité, et qu'ils l'ont comprise;
- Indiquez clairement et mettez en application les conséquences des lacunes en matière de sécurité, particulièrement lorsque des employés n'ont pas tenu compte des règles, les ont enfreintes ou ont causé du tort à votre entreprise.

En dernier lieu, le processus de licenciement d'un employé est lié à la sécurité de votre entreprise. En effet, les cas d'anciens employés qui ont accédé aux réseaux internes, volé des données et implanté des programmes malveillants sont nombreux. Lorsque l'embauche d'un employé ou d'un entrepreneur prend fin ou lorsqu'un employé ou un entrepreneur annonce son départ, l'accès de cette personne aux ordinateurs doit aussi se terminer et, ce qui est la propriété de l'entreprise, comme les ordinateurs portatifs, les clés et les laissez-passer, doit être remis — dès que possible après la fin de l'emploi.



Aide

11.1 Quand demander de l'aide

Si vous dirigez une petite ou une moyenne entreprise, vous n'avez peut-être pas à portée de main l'expertise nécessaire à la gestion de tous les aspects de la cybersécurité. Vous avez peut-être besoin d'aide pour choisir des solutions de cybersécurité et les mettre en application.

Si vous pensez ne pas être en mesure de gérer vous-même vos besoins en matière de sécurité, nous recommandons que votre entreprise cherche une aide extérieure auprès de personnes ou d'entreprises spécialisées en cybersécurité. Trouvez des entreprises ayant une bonne réputation, une bonne connaissance et une bonne expertise dans les domaines où vous avez besoin d'aide.

Par exemple, il ne serait peut-être pas pratique de gérer vous-même certaines solutions de cybersécurité, comme la sauvegarde en ligne de toutes vos données. Les entreprises spécialisées en cybersécurité peuvent fournir ce genre de service à long terme en plus d'un soutien à la clientèle, et ce, de façon plus efficace que vous le feriez.

Pour terminer, en cas de cyberattaques, il pourrait s'avérer nécessaire de prendre contact avec les autorités appropriées. Si votre entreprise ou vos employés sont menacés ou ont subi des torts au cours d'un incident lié à la cybersécurité, adressez-vous à la police. L'annexe C dresse une liste d'autres ressources que vous pourriez trouver utiles en cas de cyberattaque.

11.2 Où trouver des moyens de protection

Pour trouver ce genre d'outils de sécurité, vous devrez souvent consulter des experts et des fournisseurs externes afin de déterminer ce dont vous avez besoin et comprendre les options qui s'offrent à vous. Il existe des options gratuites, mais la plupart ont un coût de départ auquel d'autres coûts s'ajoutent par la suite.

De nombreux logiciels de sécurité gratuits sont offerts dans Internet. Cherchez toujours des commentaires que des utilisateurs ont affichés en ligne pour voir ce que d'autres ont expérimenté, parlez à d'autres propriétaires de petites entreprises et tentez de connaître la source, l'historique et la validité d'un logiciel gratuit avant de l'utiliser. Assurez-vous qu'il est largement accepté comme étant légitime et qu'il ne s'agit pas d'une forme de programme malveillant. Lorsque vous payez un logiciel de sécurité, l'appui d'un fournisseur, une garantie, un soutien technique pour l'installation et des mises à jour sont généralement inclus. Le coût peut varier grandement et peut s'échelonner sur plusieurs années, car les licences de logiciel et l'entretien sont renouvelés, souvent chaque année.

Annexes

12.1 Annexe A : Auto-évaluation de l'état de cybersécurité

Les questions qui suivent vous aideront à déterminer l'état de base de votre entreprise en ce qui a trait à la cybersécurité. En répondant à ces questions avant de lire le guide, vous serez mieux équipé pour déterminer quelles sections devraient faire l'objet d'une plus grande attention de votre part.

Elles tiennent pour acquis que votre entreprise (peu importe sa taille) :

1. Utilise des ordinateurs à des fins professionnelles;
2. Utilise des appareils informatiques et de communication mobiles à des fins professionnelles;
3. Connecte certains de ces appareils ou tous ces appareils à Internet à des fins professionnelles;
4. Peut aussi disposer d'un réseau interne employé pour l'utilisation commune de logiciels d'applications, de périphériques (comme des imprimantes) et de renseignements à l'intérieur de l'entreprise.

Pour chaque question, veuillez encercler une réponse. Si vous ne connaissez pas la réponse ou si vous ne comprenez pas la question, choisissez « Incertain ».

Faites le total de vos points en additionnant les chiffres qui sont à gauche de vos réponses. Par exemple, si vous avez répondu « Incertain », cette réponse aura la valeur zéro (0) et si vous avez répondu « Oui », la valeur sera deux (2).

Questions sur l'entreprise

1. La cybersécurité est-elle une priorité pour votre entreprise?
0. Incertain
1. Non
2. Oui

2. Quelqu'un dans votre entreprise est-il responsable de la cybersécurité?
0. Incertain
1. Non
2. Oui
3. Dans l'affirmative, est-ce un rôle permanent soutenu par la direction (encerclez si la réponse est oui)?

3. Votre entreprise a-t-elle effectué une analyse des menaces et des risques (de quelque nature que ce soit) liés à la cybersécurité?
0. Incertain
1. Non
2. Oui
3. Dans l'affirmative, les risques sont-ils classés en ordre de priorité et font-ils l'objet d'un suivi en vue de leur atténuation (encerclez si la réponse est oui)?

Annexes

4. **Votre entreprise dispose-t-elle d'un plan en matière de sécurité?**
   0. Incertain
   1. Non
   2. Oui
   3. Dans l'affirmative, est-il suivi (encerclez si la réponse est oui)?

5. **Votre entreprise dispose-t-elle d'une politique en matière de sécurité?**
   0. Incertain
   1. Non
   2. Oui
   3. Dans l'affirmative, est-elle appuyée par une formation en sensibilisation à la cybersécurité pour les employés (encerclez si la réponse est oui)?

6. **Votre entreprise dispose-t-elle d'un plan de rétablissement après une catastrophe?**
   0. Incertain
   1. Non
   2. Oui
   3. Dans l'affirmative, est-il maintenu à jour et a-t-il été testé (encerclez si la réponse est oui)?

7. **Votre organisation donne-t-elle des lignes directrices à ses employés sur le traitement et l'étiquetage des renseignements de nature délicate?**
   0. Incertain
   1. Non
   2. Oui
   3. Dans l'affirmative, les lignes directrices sont-elles appuyées par une politique ou une norme (encerclez si la réponse est oui)?

8. **Votre organisation donne-t-elle des lignes directrices à ses employés sur l'utilisation sécuritaire des appareils mobiles?**
   0. Incertain
   1. Non
   2. Oui
   3. Dans l'affirmative, ces lignes directrices sont-elles appuyées par une directive et des outils quelconques de gestion des appareils mobiles (si la réponse est oui, encerclez)?

Annexes

Questions techniques

9. **Un pare-feu est-il installé entre les ordinateurs de votre entreprise, y compris les systèmes de points de vente (PDV) et Internet?**
   0. Incertain
   1. Non
   2. Oui
   3. Dans l'affirmative, est-il entretenu par quelqu'un qui possède la formation et l'expérience appropriées (faites un cercle si la réponse est oui)?

10. **Votre entreprise utilise-t-elle un outil de chiffrement (habituellement, un logiciel) pour protéger les renseignements de nature délicate avant de les transmettre à l'extérieur de l'entreprise (par exemple, dans le cas de l'envoi de pièces jointes)?**
    0. Incertain
    1. Non
    2. Oui
    3. Dans l'affirmative, tous les membres du personnel savent-ils comment employer l'outil et son utilisation est-elle surveillée et mise en application (faites un cercle si la réponse est oui)?

11. **Votre entreprise dispose-t-elle d'un outil de filtrage ou de blocage des pourriels?**
    0. Incertain
    1. Non
    2. Oui
    3. Dans l'affirmative, tous les membres du personnel savent-ils comment signaler un pourriel menaçant ou faisant partie d'une tentative pour obtenir des renseignements personnels ou de nature délicate (faites un cercle si la réponse est oui)?

12. **Votre entreprise utilise-t-elle une protection contre les programmes malveillants?**
    0. Incertain
    1. Non
    2. Oui
    3. Dans l'affirmative, la protection est-elle installée dans tous les ordinateurs de l'entreprise et est-elle mise à jour régulièrement tous les jours ou toutes les heures (faites un cercle si la réponse est oui)?

Annexes

13. **Votre entreprise suit-elle les pratiques exemplaires consistant à utiliser des mots de passe forts et à les protéger?**
    0. Incertain
    1. Non
    2. Oui
    3. Dans l'affirmative, les règles relatives aux mots de passe forts sont-elles appliquées (faites un cercle si la réponse est oui)?

14. **Votre entreprise exécute-t-elle des sauvegardes régulières des données et des applications (habituellement, chaque jour ou plus fréquemment)?**
    0. Incertain
    1. Non
    2. Oui
    3. Dans l'affirmative, les sauvegardes sont-elles testées régulièrement et certaines sont-elles conservées à l'extérieur du site en cas de catastrophe (faites un cercle si la réponse est oui)?

15. **Votre organisation donne-t-elle des directives au personnel sur la façon de travailler de façon sécuritaire au cours de leurs déplacements ou lorsqu'ils sont à l'extérieur de l'environnement de travail?**
    0. Incertain
    1. Non
    2. Oui
    3. Dans l'affirmative, un réseau virtuel privé (RVP) est-il utilisé à cette fin (faites un cercle si la réponse est oui)?

Vous avez terminé le questionnaire d'auto-évaluation.

Si votre résultat se situe entre **0 et 15**, vous devriez lire le présent guide en entier dès que possible. Ensuite, consultez d'autres personnes de l'entreprise pour commencer à planifier et à installer des mesures de cybersécurité dans votre entreprise.

Si votre résultat se situe entre **16 et 30**, votre entreprise a fait un certain travail à l'égard de la cybersécurité. Cependant, vous devez vraisemblablement en faire davantage et lire le guide en portant une attention particulière aux domaines pour lesquels vous avez obtenu peu de points.

Si votre résultat se situe entre **31 et 45**, votre entreprise a fait de bons progrès dans plusieurs domaines de la cybersécurité. Cependant, de nouvelles menaces voient constamment le jour et il sera toujours important d'examiner les sujets de ce guide et de discuter des prochaines étapes (selon les besoins).

Annexes

12.2 Annexe B : Glossaire

Attaque : Tentative d'accéder de façon non autorisée à des renseignements professionnels ou personnels, aux systèmes informatiques ou aux réseaux à des fins (habituellement) criminelles. Une attaque réussie peut entraîner une faille de la sécurité ou être classée de façon générique, comme un « incident ».

Authentification : Mesure de sécurité mise en place (normalement au moyen de logiciels de contrôle) pour confirmer l'identité d'une personne avant de lui accorder l'accès aux services de l'entreprise, à ses ordinateurs ou à ses renseignements.

Biens : Tout ce qui appartient à l'entreprise et qui a de la valeur (y compris les renseignements sous toutes leurs formes et les systèmes informatiques).

Chiffrement : Conversion d'information en un code que seules les personnes autorisées peuvent lire, c.àd. celles qui ont reçu la « clé » (habituellement unique) et le logiciel spécial qui leur permettront de renverser le processus (déchiffrement) et d'utiliser l'information.

Correctif : Mises à jour ou réparations d'un logiciel appliquées sans qu'il soit nécessaire de remplacer le programme original en entier. Elles sont souvent fournies par le développeur de logiciels pour corriger les vulnérabilités de sécurité connues.

Cyber : Qui se rapporte aux ordinateurs, aux logiciels, aux systèmes de communications et aux services utilisés pour accéder à Internet et y interagir.

Faille : Une faille de la sécurité est une lacune qui émerge en raison d'une négligence ou d'une attaque délibérée. Elle peut aller à l'encontre d'une politique ou d'une loi et est souvent exploitée pour réaliser des actions nuisibles ou criminelles.

Hameçonnage : Genre particulier de pourriel visant une personne ou des personnes précises et que l'auteur tente de faire passer pour un message légitime dans l'intention de frauder le ou les destinataires.

HTTPS : *Hypertext Transfer Protocol Secure*.

Menace : Toutes actions ou tous évènements potentiels (délibérés ou accidentels) qui représentent un danger pour la sécurité de votre entreprise.

Mesure de protection : Processus de sécurité, mécanisme physique ou outil technique visant à lutter contre des menaces particulières. Parfois appelée contrôle.

Mot de passe : Mot secret ou combinaison de caractères utilisés pour authentifier la personne qui le détient.

OS : *Operating system* ou système d'exploitation.

Annexes

Parefeu : Genre de barrière de sécurité placée entre divers environnements réseau. Il peut s'agir d'un dispositif spécialisé ou d'un ensemble de plusieurs composantes et techniques. Seule une transmission autorisée, telle qu'elle est définie par la politique de sécurité locale, peut avoir droit de passage.

PDV : Point de vente.

PME : Petites et moyennes entreprises.

Pourriel : Courriels envoyés sans permission ni sollicitation de votre part ou de celle de l'employé à qui il a été envoyé.

Programme malveillant : Logiciel malveillant conçu et distribué pour causer des dommages. Le plus courant est le « virus ».

Risque : Exposition à des conséquences négatives si une menace était mise à exécution.

RVP : Réseau virtuel privé.

Sauvegarde : Processus consistant à copier des fichiers dans un outil de stockage secondaire afin que ces copies soient disponibles en cas de besoin pour une restauration future (p. ex. après une panne d'ordinateur).

Serveur : Ordinateur installé dans un réseau, destiné à fournir des ressources à d'autres systèmes informatiques rattachés au réseau (il stocke et « sert » des données et des applications).

URL : *Uniform Resource Locator* (localisateur uniforme de ressources).

Vol d'identité : Copie des renseignements personnels d'une autre personne (comme son nom, son numéro d'assurance sociale) pour ensuite se faire passer pour elle et commettre une fraude ou une autre activité criminelle.

Vulnérabilité : Faiblesse des logiciels, du matériel, de la sécurité matérielle ou pratique humaine pouvant être exploitée pour commettre des attaques à la sécurité.

WiFi : Réseau local (RL) qui emploie des signaux radio pour transmettre et recevoir des données à des distances de quelques centaines de mètres.

Annexes

12.3 Annexe C : Sites Web et coordonnées liés à la cybersécurité canadienne

12.3.1 Sites du gouvernement du Canada liés à la cybersécurité

1. **Le site Pensez cybersécurité** offre des nouvelles, des conseils et des directives sur la cybersécurité pour les particuliers et les entreprises au Canada
   - http://www.PensezCybersecurite.gc.ca

2. **Le Centre antifraude du Canada pour la prévention et la déclaration des fraudes** (y compris le cybercrime)
   - Ligne téléphonique sans frais : 1-888-495-8501
   - Télécopieur sans frais : 1-888-654-9426
   - Courriel : info@antifraudcentre.ca
   - http://www.antifraudcentre-centreantifraude.ca/francais/home.html

3. **Le site du Conseil de la radiodiffusion et des télécommunications canadiennes où vous pouvez déclarer les pourriels par téléphone**
   - http://www.crtc.gc.ca/fra/INFO_SHT/G9.htm.

4. **Le site du Commissariat à la protection de la vie privée du Canada**
   - Outil d'auto-évaluation de la protection des renseignements personnels : http://www.priv.gc.ca/resource/tool-outil/security-securite/francais/AssessRisks.asp?x=1
   - Un programme de gestion de la protection de la vie privée : la clé de la responsabilité : http://www.priv.gc.ca/information/guide/2012/gl_acc_201204_f.asp

5. **La Loi canadienne anti-pourriel**
   - http://fightspam.gc.ca/eic/site/030.nsf/fra/home
   - Le pourriel vous inquiète? Cinq choses à surveiller : http://fightspam.gc.ca/eic/site/030.nsf/fra/h_00241.html

Annexes

12.3.2 Associations membres d'organismes de cybersécurité œuvrant au Canada

Les associations du secteur de la cybersécurité constituent une bonne source de renseignements et de conseils détaillés sur la cybersécurité des petites et moyennes entreprises. Elles peuvent également formuler des recommandations sur les fournisseurs de services dans votre secteur, si vous avez besoin d'aide.

Ces sites sont offerts uniquement en anglais.

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