



LE GUIDE PENSEZ CYBERSÉCURITÉ POUR LES PETITES ENTREPRISES



D96-87/1-2024F-PDF 978-0-660-69583-9



Centre de la sécurité des
télécommunications Canada

Communications Security
Establishment Canada

[PENSEZCYBERSECURITE.CA](https://www.pensezcybersecurite.ca)

Canada

INTRODUCTION

Une enquête menée par la Chambre de commerce de la Colombie-Britannique a révélé que près des deux tiers (61 %) des entreprises canadiennes ont déjà été confrontées à un incident de cybersécurité¹. Cela est énorme!

Un incident de cybersécurité peut prendre plusieurs formes. Vous pouvez par exemple être victime d'une attaque par hameçonnage visant à dérober des renseignements commerciaux, télécharger à votre insu un rançongiciel ou encore voir votre accès bloqué aux comptes de médias sociaux de votre entreprise.

Lorsque Pensez cybersécurité a demandé aux gestionnaires de petites entreprises quelles étaient les cybermenaces qui les préoccupaient le plus, ceux-ci ont répondu qu'ils craignaient qu'une cybermenace entraîne des interruptions de travail, des pertes financières, une atteinte à la réputation de leur entreprise ou que leurs données ne fassent l'objet d'une demande de rançon².

Les entreprises confrontées à des failles de cybersécurité ne sont pas seulement touchées financièrement, elles peuvent également perdre la confiance de leurs fournisseurs et de leurs clients.



Mise au point

Les comptes de votre petite entreprise sont-ils bien sécurisés? Répondez aux dix questions de l'**examen Pensez cybersécurité** pour le découvrir.



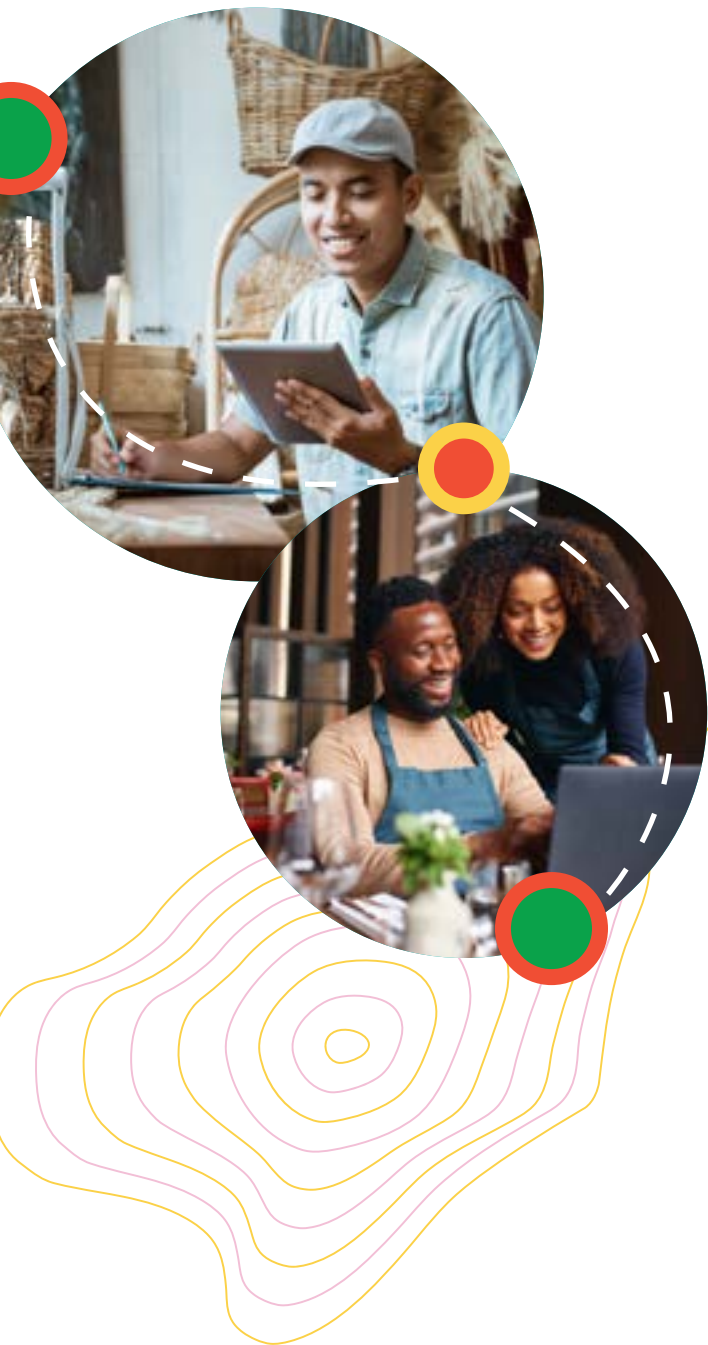
MAGASIN

OUVERT

Si vous êtes propriétaire d'une petite entreprise, ce guide a été conçu pour vous.

¹Enquête sur la cybersécurité et les entreprises, Chambre de commerce de la Colombie-Britannique : <https://bccchamber.org/news/new-cyber-security-and-business-survey-reveals-majority-businesses-have-experienced-cyber> (disponible en anglais seulement)

²Enquête de suivi sur la sensibilisation à la cybersécurité, EKOS Research Associates, 2021.



À qui s'adresse ce guide?

Le guide Pensez cybersécurité est conçu pour les petites entreprises :

- qui n'ont pas d'équipe consacrée aux technologies de l'information (TI);
- qui utilisent les médias sociaux pour promouvoir leurs activités et interagir avec leurs clients;
- qui utilisent une plateforme de commerce électronique pour réaliser des ventes;
- qui recherchent des mesures simples pour assurer la sécurité de leur entreprise en ligne.



Ce que vous trouverez dans ce guide

Ce guide explique les mesures que vous pouvez prendre pour atténuer les risques de cybermenaces et mieux protéger votre entreprise. Ces mesures contribueront à sécuriser les biens, les données sensibles et les investissements de votre entreprise.

Les cybermenaces courantes	5
Prioriser la cybersécurité	6
Budgétiser la cybersécurité	7
La cyberassurance	8
Dix mesures pour atténuer les risques	9
1. Dresser l'inventaire des biens	10
2. Sécuriser les comptes et appareils	11
3. Sécuriser le réseau	16
4. Développer un système de sauvegarde	18
5. Protéger les clients et les données sensibles	19
6. Activer les mises à jour automatiques .	20
7. Élaborer un plan de cybersécurité	21
8. Former les employés	23
9. Établir un plan d'intervention en cas d'incident	25
10. Se tenir au fait en matière de cybersécurité	27
Conclusion	28
Ressource 1 : Plan de cybersécurité	
Ressource 2 : Liste d'inventaire des biens	
Ressource 3 : Plan d'intervention en cas d'incident	



LES CYBERMENACES COURANTES

En tant que chef d'entreprise, il est important de connaître les cybermenaces courantes et de comprendre les façons d'empêcher ces attaques d'avoir une incidence négative sur votre entreprise.

L'hameçonnage : cyberattaque par laquelle un criminel tente de vous inciter à cliquer sur un lien malveillant, télécharger un logiciel malveillant ou partager des renseignements sensibles, et ce, par téléphone, par message texte, par courrier électronique, ou encore par le biais des médias sociaux. Les tentatives d'hameçonnage se présentent souvent comme des messages légitimes provenant d'une source fiable (par exemple, d'une banque ou d'une société de messagerie), mais le plus souvent il s'agit de messages de masse génériques.



Pour plus d'informations, consultez la publication du Centre canadien pour la cybersécurité : **Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage - ITSAP.00.101.**

Le piratage psychologique : type d'attaque par hameçonnage ciblé par lequel un cybercriminel effectue des recherches sur les moteurs de recherche et les médias sociaux pour en savoir plus sur vous ou votre entreprise. Il vous envoie ensuite un message qui semble provenir d'un collègue, d'un fournisseur, d'une entreprise familière ou d'une autre source fiable. Il vous incite à partager des renseignements sensibles, comme des mots de passe, des numéros de carte de crédit ou des données financières.



Pour plus d'informations, consultez la publication du Centre canadien pour la cybersécurité : **Reconnaître les courriels malveillants (ITSAP.00.100).**

Les maliciels : les cybercriminels peuvent utiliser des logiciels malveillants (maliciels) pour infiltrer ou endommager vos réseaux, vos systèmes et vos appareils. Une fois le maliciel installé dans les systèmes et les appareils de votre entreprise, les cybercriminels peuvent facilement accéder aux renseignements sensibles.



Pour plus d'informations, consultez la publication du Centre canadien pour la cybersécurité : **Protéger votre organisation contre les maliciels (ITSAP.00.057).**

Les rançongiciels : type de logiciel malveillant qui infecte vos appareils et exige une rançon en échange de vos fichiers et de vos données. L'appareil infecté affiche un message expliquant que vos fichiers sont inaccessibles et que vous devez payer pour récupérer vos informations. Mais contrairement aux kidnappeurs dans les films, au lieu d'une valise pleine d'argent, les cybercriminels exigent un paiement sous la forme d'une monnaie numérique difficile à retracer, comme le bitcoin.



Pour plus d'informations, consultez la publication du Centre canadien pour la cybersécurité : **Rançongiciels : comment les prévenir et s'en remettre (ITSAP.00.099).**

Le piratage : terme utilisé pour décrire les actions entreprises par les criminels pour obtenir un accès non autorisé à vos appareils. Avec cet accès, les pirates peuvent prendre le contrôle, par exemple, des comptes de médias sociaux de votre entreprise pour accéder à des renseignements personnels et professionnels, rediriger vos abonnés vers des activités frauduleuses ou jeter le discrédit sur votre entreprise.



Pour plus d'informations, consultez les publications du Centre canadien pour la cybersécurité : **Êtes-vous victime de piratage? - ITSAP.00.015** et **Perte de contrôle des comptes de médias sociaux.**



Retour à la table des matières

PRIORISER LA CYBERSÉCURITÉ

DÉFINIR LES RÔLES ET LES RESPONSABILITÉS

Il devrait y avoir au moins une personne responsable de la cybersécurité au sein de votre entreprise, dont les tâches incluent :

- s'informer sur les menaces, les tendances et les options en matière de cybersécurité;
- planifier, mettre en œuvre et maintenir les dix mesures d'atténuation décrites dans ce guide;
- aider les autres membres du personnel à comprendre les pratiques exemplaires et les politiques en matière de cybersécurité.

Grâce à ce guide, la personne responsable de la cybersécurité de votre entreprise disposera des connaissances et des outils nécessaires pour protéger votre entreprise contre les cybermenaces les plus courantes.



EXTERNALISER LA CYBERSÉCURITÉ

Certaines petites entreprises souhaitent faire appel à des prestataires de services pour gérer à distance leur infrastructure informatique, leur cybersécurité et d'autres opérations commerciales connexes.



Pour plus d'informations sur la collaboration avec les fournisseurs de services gérés et pour connaître la meilleure option pour votre entreprise, consultez la publication du Centre canadien pour la cybersécurité : **Choisir la solution de cybersécurité qui convient le mieux à votre organisation - ITSM.10.023.**



Retour à la table des matières

BUDGÉTISER LA CYBERSÉCURITÉ

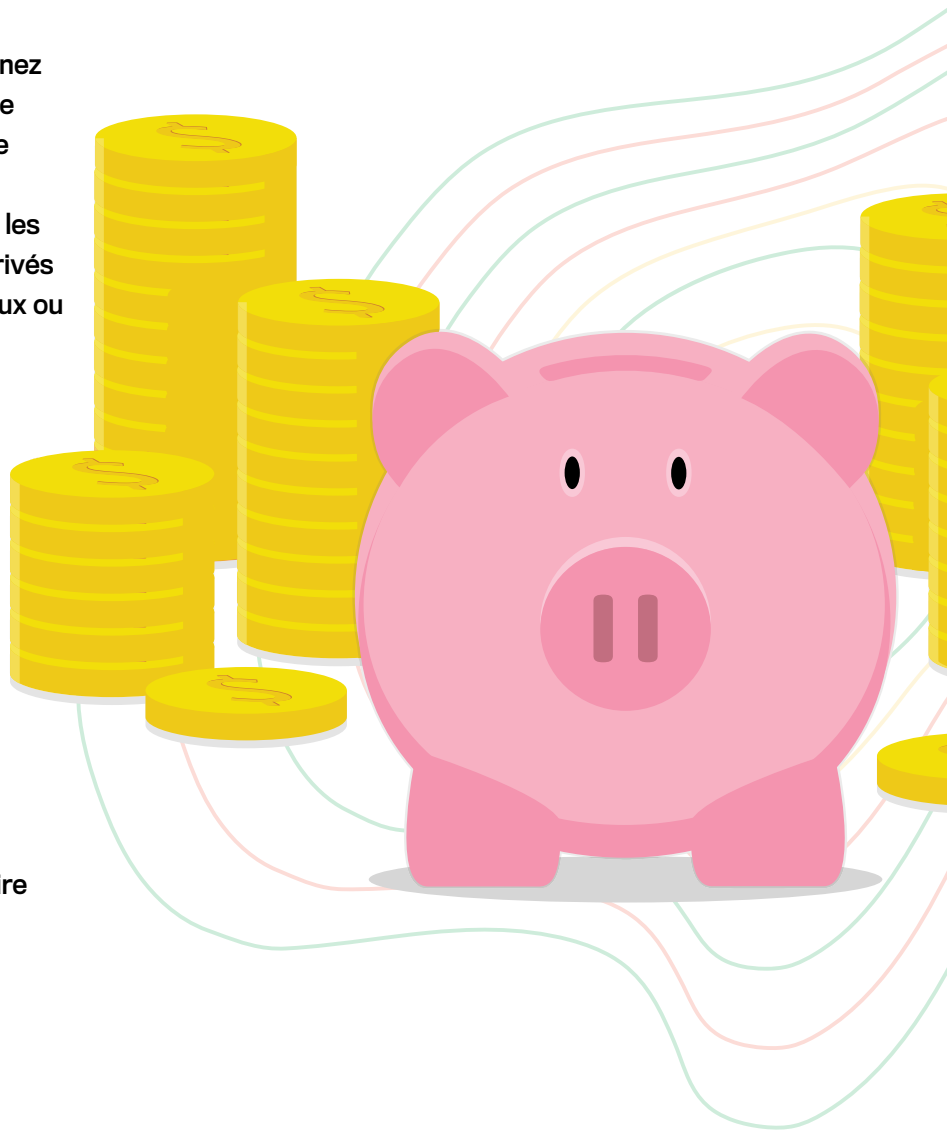
Assurer la cybersécurité de votre entreprise peut demander un investissement financier selon les outils que vous choisissez de mettre en place. Tenez compte des coûts liés à la cybersécurité lors de l'élaboration de vos plans d'entreprise et de votre budget annuel. Par exemple, les applications et services suivants, tels que les logiciels antivirus, les gestionnaires de mots de passe et les réseaux privés virtuels (RPV), peuvent engendrer des frais initiaux ou des abonnements annuels.

Pour éviter les dépenses imprévues, il est préférable de se préparer aux coûts associés aux éléments suivants :

- ✓ outils de sécurité
- ✓ mises à niveau ou mises à jour
- ✓ soutien technique
- ✓ coûts de formation
- ✓ imprévus

Les fonds d'urgence deviennent un atout pour faire face à des situations imprévues (par exemple, une infection par maliciel).

Dans certains cas, votre assurance peut couvrir les pertes dues à un incident de cybersécurité. Il est important de discuter au préalable de votre couverture avec votre assureur.



[Retour à la table des matières](#)



Pour de plus amples renseignements sur la cyberassurance, consultez la publication du Bureau d'assurance du Canada sur Pensez cybersécurité : **Votre petite entreprise a-t-elle besoin d'une cyberassurance?**



LA CYBERASSURANCE

La cyberassurance est un produit spécialisé destiné à aider les entreprises à gérer les pertes causées par les attaques de réseaux informatiques, telles que le vol de données et la cyberextorsion. La cyberassurance peut couvrir toute une série de cyberévénements, notamment :

- le vol de données confidentielles (la perte et l'accès non autorisé à des informations confidentielles ou personnelles);
- la cyberextorsion (une demande de paiement sous la menace de restreindre votre accès ou de compromettre vos données, comme dans le cas d'une attaque par rançongiciel);
- des perturbations technologiques (une défaillance technologique ou une attaque par déni de service qui empêche l'accès à vos services en ligne).

La cyberassurance peut aider à couvrir certains frais découlant d'une cyberattaque, notamment la représentation juridique, l'avis aux parties touchées, l'embauche d'une entreprise pour enquêter sur la cause de la faille de sécurité et la restauration des données endommagées ou corrompues.



[Retour à la table des matières](#)

DIX MESURES POUR ATTÉNUER LES RISQUES

Voici dix mesures à prendre pour renforcer la cybersécurité de votre entreprise. Ces mesures ne sont pas classées par ordre d'importance, mais offrent des conseils en matière de cybersécurité pour les différents secteurs de votre entreprise. Tenez compte des étapes suivantes lors de la mise en œuvre et des améliorations apportées à la cybersécurité de votre entreprise.



1 Dresser l'inventaire des biens

6 Activer les mises à jour automatiques

2 Sécuriser les comptes et appareils

7 Élaborer un plan de cybersécurité

3 Sécuriser le réseau

8 Former les employés

4 Développer un système de sauvegarde

9 Établir un plan d'intervention en cas d'incident

5 Protéger les clients et les données sensibles

10 Se tenir au fait en matière de cybersécurité



[Retour à la table des matières](#)

1

DRESSER L'INVENTAIRE DES BIENS

Dresser l'inventaire de vos biens est une première étape importante pour protéger votre entreprise contre les cybermenaces. Dressez une liste de tous les biens de votre entreprise afin d'en assurer le suivi et d'en gérer l'utilisation en cas d'incident de cybersécurité. Voici quelques exemples de biens courants pour lesquels vous devriez dresser un inventaire :

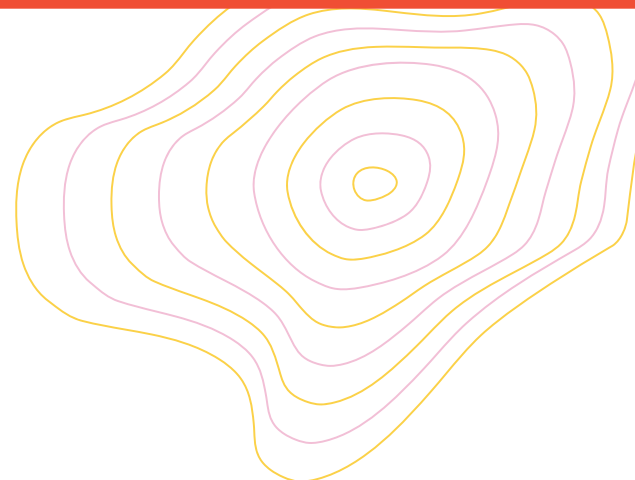
- les **appareils physiques** utilisés par votre entreprise pour se connecter à Internet, comme les ordinateurs de bureau, les ordinateurs portables, les serveurs, les routeurs et les appareils mobiles, tels que les téléphones et les tablettes;
- les **périphériques physiques**, tels que les imprimantes, les numériseurs, les moniteurs, les claviers, les souris et les stations d'accueil;
- les **appareils connectés ou intelligents**, tels que les systèmes de points de vente (PDV), les thermostats, les assistants personnels, les haut-parleurs et les systèmes d'éclairage et de sécurité;
- les **dispositifs de stockage physique**, tels que les disques durs externes, les dispositifs de stockage en réseau et les clés USB;
- les **biens et services numériques** (comptes de médias sociaux, sites Web, services de comptabilité en nuage et en ligne).

Votre liste d'inventaire des biens doit inclure les numéros de série de chaque appareil, leur emplacement, les dates d'expiration des licences de logiciels, ainsi que les noms et les coordonnées des personnes qui y ont accès.



Modèle

Vous pouvez trouver un modèle de liste d'inventaire des biens **à la fin de ce guide.**



SÉCURISER LES COMPTES ET APPAREILS

Une fois que vous avez dressé l'inventaire de vos biens, envisagez les mesures de cybersécurité suivantes pour sécuriser les appareils et les comptes utilisés dans le cadre de vos activités commerciales.

Appareils

Si vous utilisez plusieurs appareils, tels que des ordinateurs de bureau, des ordinateurs portables, des téléphones mobiles et des tablettes pour gérer votre entreprise, tenez compte des éléments suivants :

- Quels sont les appareils qui ont accès aux données des clients (par exemple, noms, adresses, informations de paiement)?
- Quels sont les appareils qui ont accès aux données financières de votre entreprise (par exemple, comptes bancaires, renseignements fiscaux)?
- Quels sont les appareils qui ont accès aux données relatives à votre avantage concurrentiel (par exemple, les prix, les marges de profit et les brevets)?
- Vos employés utilisent-ils leurs propres appareils pour accéder aux renseignements de votre entreprise?

N'oubliez pas que votre entreprise ne peut gérer les appareils personnels des employés de la même manière que les appareils appartenant à l'entreprise. Les données de votre entreprise sont sensibles aux vulnérabilités des appareils des employés, qui peuvent inclure des maliciels, des logiciels obsolètes et l'absence d'outils de sécurité.

En fournissant à ses employés des appareils appartenant à l'entreprise, votre organisation peut en gérer l'utilisation et s'assurer ainsi que des mesures de cybersécurité sont mises en place.

S'il n'est pas possible de fournir des appareils à tous vos employés, veillez à définir les activités professionnelles qui peuvent être effectuées au moyen des appareils personnels.

Si votre entreprise autorise ses employés à utiliser leurs appareils personnels pour traiter des renseignements commerciaux, n'oubliez pas de supprimer l'accès au compte de l'entreprise lorsqu'un employé quitte votre organisation. Pour ce faire, vous pouvez élaborer une politique « Prenez vos appareils personnels (PAP) » qui décrit les activités professionnelles que les employés sont autorisés à effectuer sur leurs appareils personnels.



Pour plus de détails sur la politique PAP, consultez la publication du Centre canadien pour la cybersécurité : **Sécurité des appareils des utilisateurs finaux pour les modèles de déploiement Prenez vos appareils personnels (PAP) - ITSM.70.003.**



Retour à la table des matières



Accès, comptes et rôles

Veillez à ce que l'accès aux programmes, aux logiciels et aux données sensibles soit limité aux personnes qui en ont réellement besoin dans le cadre de leurs activités professionnelles. Cette restriction d'accès peut se faire à même le logiciel ou encore par l'intermédiaire du système d'exploitation, ce qui est particulièrement important pour l'accès des administrateurs. Limiter l'accès permet de réduire les risques.

Réduisez au minimum le nombre d'employés disposant de privilèges administratifs sur les logiciels, en particulier sur les applications importantes et les dispositifs de sécurité. Les cybercriminels ciblent les comptes d'utilisateurs disposant de privilèges d'administration, puisqu'ils leur donnent un haut niveau de contrôle sur les logiciels et les systèmes.



Pour plus de détails, consultez la publication du Centre canadien pour la cybersécurité : **Gestion et contrôle des privilèges administratifs (ITSAP.10.094)**.

Les comptes de médias sociaux et autres services en ligne vous permettent souvent d'attribuer des rôles aux employés au sein du compte de votre entreprise. Par exemple, Facebook propose des rôles d'administrateur, d'éditeur, de modérateur, de gestionnaire d'emplois, d'annonceur et d'analyste. Ces rôles sont assortis d'accès et d'autorisations spécifiques. Votre entreprise peut utiliser ces rôles pour contrôler l'accès aux données des clients et aux données financières.

Mots de passe et phrases de passe

La plupart des appareils viennent avec un nom d'utilisateur et un mot de passe définis par défaut par le fabricant. Cela représente un risque de sécurité important pour votre entreprise, mais ce problème peut être facilement résolu en **changeant le mot de passe** dès que vous recevez un nouvel appareil. Dans la mesure du possible, utilisez une phrase de passe, qui est une combinaison d'au moins quatre mots aléatoires d'une longueur minimale de 15 caractères. Une phrase de passe doit être facile à retenir pour vous, mais difficile à deviner pour un cybercriminel.

Si votre appareil ou votre compte ne permet pas d'utiliser une phrase de passe longue, choisissez un mot de passe composé d'au moins douze caractères comprenant une combinaison de lettres majuscules et minuscules, au moins un chiffre et au moins un caractère spécial qui n'est ni une lettre ni un chiffre.

Il est important d'utiliser des mots de passe uniques pour chaque appareil et chaque compte au sein de votre entreprise. Ainsi, si un appareil ou un compte est compromis, les autres comptes et appareils ne seront pas aussi facilement accessibles.



Retour à la table des matières

Gestionnaires de mots de passe

Si l'utilisation d'un mot de passe unique pour chaque appareil et chaque compte permet d'éviter que d'autres comptes et appareils soient compromis, cela veut dire qu'il faut se rappeler d'un grand nombre de mots de passe! Utilisez un gestionnaire de mots de passe pour vous aider à créer, organiser et mémoriser vos informations d'identification.



Pour plus d'informations, consultez la publication de Pensez cybersécurité : **Comment choisir le gestionnaire de mots de passe qui vous convient.**

Authentification multifactorielle (AMF)

Activez l'authentification multifactorielle (AMF) pour tous les comptes où elle est offerte. Il s'agit d'une combinaison de deux facteurs d'authentification ou plus. Les facteurs d'authentification peuvent être une combinaison de ce que l'utilisateur connaît (par exemple, un mot de passe ou un code NIP), possède (par exemple, une carte à puce ou une clé de sécurité), ou représente (des caractéristiques biométriques telles qu'une empreinte digitale ou la reconnaissance faciale). L'utilisation d'un facteur d'authentification supplémentaire pour vérifier l'identité des utilisateurs garantit que même si un cybercriminel met la main sur un mot de passe, il ne pourra pas accéder au compte sans connaître les facteurs d'authentification supplémentaires. Pour plus de détails sur la mise en place de l'AMF, consultez la publication du Centre canadien pour la cybersécurité : **Étapes à suivre pour déployer efficacement l'authentification multifactorielle (AMF) - ITSAP.00.105.**



Appareils intelligents et Internet des objets (IdO)


L'Internet des objets désigne le réseau d'appareils quotidiens compatibles avec le Web, capables de se connecter et d'échanger des informations. Ces appareils intelligents comprennent les appareils personnels de suivi de la condition physique, les téléviseurs, les thermostats ou les voitures connectés.

Lorsque vous choisissez des appareils intelligents pour votre petite entreprise, tenez compte des caractéristiques de sécurité et de la politique de confidentialité de l'appareil.

➤ **Caractéristiques de sécurité** : certains fabricants d'appareils intelligents conçoivent leurs produits pour qu'ils soient faciles à utiliser et peu coûteux pour le consommateur. Mais cela peut signifier que les fonctions de sécurité de l'appareil sont faibles ou inexistantes. À l'achat d'un nouvel appareil intelligent, réfléchissez aux données qui seront transmises par l'appareil, puis déterminez comment l'appareil peut protéger ces données. Au minimum, vérifiez si l'appareil vous offre la possibilité de créer votre propre phrase de passe ou mot de passe robuste et unique.

➤ **Politique de confidentialité** : les appareils intelligents peuvent capter et transmettre bon nombre de renseignements personnels sur votre entreprise, y compris des données de paiement. Par conséquent, avant d'acheter un appareil intelligent, vérifiez auprès du fournisseur comment la confidentialité de vos renseignements sera assurée. Les fournisseurs d'appareils intelligents dignes de confiance publieront une politique expliquant les types de données que leur appareil recueillera sur vous, la manière dont ils protégeront la confidentialité de vos données et les entreprises et annonceurs avec lesquels ils partageront vos données. Veillez donc à consulter et à comprendre la politique de confidentialité et les conditions d'utilisation de chaque fournisseur.





Pour plus d'informations, consultez les publications suivantes du Centre canadien pour la cybersécurité : **Sécurité de l'Internet des objets (IdO) - ITSAP.00.012** et **Est-ce que votre appareil intelligent vous écoute? (ITSAP.70.013)**.

Logiciels et applications

La sécurité des logiciels et des applications utilisés par votre entreprise est primordiale pour maintenir un bon niveau de cybersécurité. Les logiciels peuvent présenter des problèmes (généralement connus sous le nom de « bogues ») qui les rendent peu fiables. Ces bogues peuvent être exploités par des pirates et leur permettre trop facilement d'accéder à vos informations. Les logiciels peuvent parfois contenir des logiciels malveillants, communément appelés « maliciels ». Pour maintenir la sécurité des logiciels :

- utilisez des logiciels légitimes qui ont été testés et qui proviennent de fournisseurs dignes de confiance;
- n'utilisez pas de versions non autorisées de logiciels téléchargés illégalement;
- appliquez les mises à jour de sécurité sur votre logiciel dès qu'elles sont offertes (voir **l'étape 6 pour activer les mises à jour automatiques**).



Hébergement de sites Web

Si le site Web de votre entreprise n'est pas correctement sécurisé, il pourra être facilement compromis. Cela pourrait entraîner des actes de vandalisme, des interruptions de service ou le vol de données de l'entreprise ou de vos clients. La sécurité des sites Web varie d'une entreprise à l'autre, mais voici tout de même quelques conseils de base à suivre :

- Si votre entreprise utilise un service d'hébergement Web, assurez-vous que celui-ci dispose d'un plan de sécurité et qu'il :
 - analyse les serveurs Web et votre site Web à la recherche de problèmes potentiels, puis corrige ces problèmes afin de mieux protéger le serveur et votre site;
 - surveille votre site Web (et tous les systèmes) pour détecter toute intrusion ou tentative de vandalisme;
 - protège votre site Web contre les intrusions et les perturbations;
 - rétablira votre site Web en cas de panne ou d'interruption de service par des cybercriminels.
- Utilisez des adresses courriel professionnelles génériques telles que `ventes@votreentreprise.com` pour empêcher les cybercriminels d'accéder à des renseignements personnels (par l'entremise du nom de l'adresse courriel ou d'une attaque par hameçonnage).
- Si vous hébergez votre site Web à l'interne sur des serveurs appartenant à votre entreprise, consultez la publication du Centre canadien pour la cybersécurité : **Facteurs à considérer en matière de cybersécurité pour votre site Web (ITSM.60.005)**.





Sécurité des points de vente (PDV)

Il est probable que votre entreprise s'appuie sur des systèmes électroniques de point de vente (PDV) pour traiter les transactions financières. Les clients s'attendent à ce que les PDV leur permettent d'effectuer des transactions instantanées par carte de débit ou de crédit, ce qui en fait un élément essentiel de vos activités commerciales.

Vos systèmes de PDV peuvent être un autre moyen pour les cybercriminels d'accéder à vos réseaux informatiques, c'est pourquoi il est très important de les protéger. Les cybercriminels peuvent pirater les systèmes de PDV (en utilisant des identifiants volés ou des vulnérabilités non corrigées) pour voler les numéros de cartes et les numéros d'identification personnels (NIP) qui y sont associés, qu'ils peuvent ensuite utiliser pour accéder aux comptes de vos clients.

Voici les mesures que vous pouvez prendre pour améliorer la sécurité des PDV afin de protéger vos clients et votre entreprise :

- Veillez à ce que vos systèmes de PDV soient protégés par un pare-feu.
- Mettez en place un logiciel de cryptage fort pour la transmission de toutes les données (par exemple, les données des titulaires de cartes) entre votre système de PDV et le fournisseur de services de PDV.
- Vérifiez que votre fournisseur de services a établi cette protection par défaut.
- Si vous n'êtes pas certain de la marche à suivre, demandez l'aide de votre fournisseur de services de PDV ou d'un consultant en cybersécurité (ayant de l'expérience dans le domaine des PDV).
- Remplacez le nom d'utilisateur et le mot de passe par défaut par un nouveau nom d'utilisateur et un nouveau mot de passe uniques.
- Limitez toujours l'accès aux données des clients aux employés qui ont besoin d'y accéder et qui sont autorisés à le faire.
- Maintenez votre logiciel antivirus et antimaliciel à jour.



[Retour à la table des matières](#)

SÉCURISER LE RÉSEAU

Les cybercriminels peuvent faire des ravages dans les entreprises en attaquant votre réseau pour voler des données et se livrer à d'autres activités malveillantes. Assurez-vous que votre réseau est à tout le moins protégé par un pare-feu et un logiciel antivirus. Vous devriez également envisager de segmenter votre réseau pour mieux protéger vos systèmes et vos données. Si vous ou vos employés télétravaillez ou voyagez pour le travail, fournissez une connexion à un réseau privé virtuel (RPV) pour utiliser les ressources de l'entreprise à distance.



Pour plus de détails sur la sécurisation de votre réseau, consultez les publications du Centre canadien pour la cybersécurité : **Les réseaux privés virtuels (ITSAP.80.101)** et **Les 10 mesures de sécurité des TI : no 5, Segmenter et séparer l'information - ITSM.10.092.**

Réseau Wi-Fi privé

Sécuriser le réseau Wi-Fi de votre entreprise est plus simple que vous ne le croyez. Commencez par modifier le nom et le mot de passe Wi-Fi fournis avec votre routeur. Veillez à ce que le nom du réseau ne contienne aucune information personnelle et utilisez un mot de passe ou une phrase de passe unique et difficile à deviner. Créez ensuite un réseau Wi-Fi distinct pour les invités et les appareils intelligents. Cela ajoute une couche de protection supplémentaire à votre réseau plus sensible, puisque les appareils intelligents sont souvent plus vulnérables aux cybermenaces.



Réseau Wi-Fi public

Les appareils de votre entreprise et les renseignements qu'ils contiennent sont particulièrement vulnérables lorsque vous travaillez en dehors du bureau ou de votre domicile. Plusieurs hôtels, cafés, centres de conférence et autres lieux publics proposent une connexion Wi-Fi souvent gratuite, mais peu sécuritaire.

Évitez les connexions Wi-Fi offertes à tous et gratuites, à moins qu'elles ne soient sécurisées par un mot de passe et un système de cryptage. Même dans ce cas, soyez prudent lorsque vous partagez des renseignements sensibles. Si une connexion Wi-Fi non cryptée doit être utilisée, les documents professionnels et les courriels ne doivent pas être transmis, à moins d'utiliser un réseau privé virtuel (RPV) professionnel. Le RPV permettra de crypter les informations transmises.



Pour plus de détails sur la façon d'effectuer ces changements, consultez la publication de Pensez cybersécurité : **Votre réseau est-il prêt à tout?**



Réseau privé virtuel (RPV)

Un RPV peut aider à sécuriser les informations de votre entreprise entre vos appareils et Internet. Il est également très utile pour sécuriser les données utilisées sur des appareils et des systèmes à distance. La nature ultraconnectée de la vie d'aujourd'hui a rendu possible le travail à distance, mais les réseaux domestiques ne sont pas aussi sécurisés que les réseaux d'entreprise. Si vous et vos employés faites du télétravail, quel que soit le lieu, protégez les données et le réseau de votre entreprise en utilisant un réseau privé virtuel (RPV). La connexion à un réseau ouvert à tous ou non sécurisé par l'intermédiaire d'un RPV ajoute une couche de cryptage supplémentaire pour protéger la confidentialité de vos informations. Les RPV peuvent se présenter sous la forme d'extensions de navigateur, d'applications pour appareils ou encore faire partie intégrante de votre routeur. Effectuez des recherches pour savoir quel type de RPV convient le mieux à vos besoins.

Logiciel antivirus

Les logiciels antivirus analysent les fichiers, les courriels et les téléchargements avant qu'ils n'atteignent vos appareils. Ils peuvent ainsi protéger vos appareils contre les maliciels. Pensez à choisir un logiciel qui identifie les sites Web potentiellement malveillants, tout en surveillant et en signalant les programmes suspects. Vous pouvez ainsi vous

protéger des signatures de logiciels malveillants nouvelles ou inconnues. Bien qu'il existe de nombreuses versions gratuites de logiciels antivirus disponibles en ligne, il peut être intéressant d'investir dans un logiciel payant de qualité pour votre entreprise. Configurez le logiciel antivirus pour qu'il effectue des analyses régulières, y compris en dehors des heures de travail. Les logiciels antivirus peuvent ainsi éliminer les menaces connues et contribuer à la sécurité de vos appareils et de votre réseau.



Pour plus d'informations, consultez la publication de Pensez cybersécurité : **Comment évaluer les logiciels antivirus (et choisir celui qui vous convient!)**.

Pare-feu

Un pare-feu est un dispositif de sécurité qui permet de protéger votre réseau, vos appareils et vos données en bloquant le trafic indésirable et les logiciels malveillants. De nombreux systèmes d'exploitation sont dotés de pare-feu logiciels intégrés. Si ce n'est pas le cas, effectuez des recherches et procurez-vous un logiciel pare-feu auprès d'une entreprise réputée. Pour une protection supplémentaire, vous pouvez utiliser un pare-feu matériel, tel que celui qui est intégré à un routeur. Consultez les ressources en ligne du fabricant de votre routeur pour savoir comment configurer ces paramètres de pare-feu.

Selon la taille de votre entreprise, vous pouvez également bénéficier d'un service gratuit de pare-feu du système de noms de domaine (DNS), offert par le Bouclier canadien de CIRA, qui assure la protection de la vie privée et la sécurité en ligne.



Pour plus d'informations consultez la publication de Pensez cybersécurité : **Le Bouclier canadien de CIRA : Enfiler votre armure de cybersécurité.**



DÉVELOPPER UN SYSTÈME DE SAUVEGARDE



Il est essentiel d'effectuer des sauvegardes de toutes vos données, puisque cela permet de récupérer rapidement les données endommagées ou perdues à la suite d'un accident, d'une catastrophe naturelle ou d'une cyberattaque. Dans le cas d'une attaque par rançongiciel, où les données et les systèmes de votre entreprise sont verrouillés jusqu'à ce qu'une rançon soit payée, une sauvegarde peut éviter à votre entreprise une perte importante de données et d'argent. Vos données doivent être sauvegardées sur plusieurs systèmes afin de garantir qu'elles sont bien sécurisées et faciles à récupérer. Voici quelques exemples d'options courantes pour le stockage des sauvegardes :

- **Le stockage en nuage** permet d'enregistrer vos fichiers, documents et photos dans une base de données distante. Un service de stockage en nuage peut être fourni avec votre ordinateur ou votre appareil. Toutefois, pour une entreprise, il vaut souvent la peine d'investir dans une capacité de stockage supplémentaire. Certains services de stockage en nuage peuvent également offrir une récupération historique des fichiers ou une protection contre les rançongiciels.
- **Les disques durs externes** sont des dispositifs qui peuvent être connectés à votre ordinateur ou à votre appareil pour sauvegarder une copie de fichiers, de documents et de photos. Connectez régulièrement votre disque dur externe pour y sauvegarder vos fichiers.
- **Le stockage externe** peut également se faire sur un périphérique de stockage en réseau (NAS) ou sur une clé USB.

Astuce



Gardez à l'esprit que la meilleure **sauvegarde** est celle qui possède sa propre sauvegarde. Même si vous utilisez un service en nuage, sauvegardez vos données les plus importantes sur un périphérique de stockage externe secondaire.

Protégez votre système de sauvegarde à l'aide de mots de passe forts et d'un système de cryptage. Lorsqu'ils ne sont pas utilisés, les dispositifs externes doivent être stockés dans des endroits à l'abri des intempéries et des accès non autorisés. N'oubliez pas de déconnecter les périphériques de stockage externes lorsque la sauvegarde est terminée. Configurez les sauvegardes de manière qu'elles s'effectuent automatiquement ou fixez-vous des rappels pour sauvegarder vos données sur des périphériques externes au moins une fois par semaine. Testez régulièrement vos méthodes de sauvegarde pour vous assurer qu'elles fonctionnent et que la récupération se fait sans heurts. Il est important que la récupération s'effectue facilement pour que votre entreprise puisse fonctionner en toute sécurité et sans retards dus à des incidents.



[Retour à la table
des matières](#)

PROTÉGER LES CLIENTS ET LES DONNÉES SENSIBLES

Une faille de vos systèmes de cybersécurité pourrait entraîner la perte des données de vos clients. Cela pourrait coûter à votre entreprise la confiance et la réputation qu'elle s'est efforcée d'acquérir. Les données des clients et les données sensibles peuvent inclure :

- les données relatives aux clients (p. ex. noms, adresses, informations de paiement);
- les données financières (p. ex. comptes bancaires, informations fiscales);
- les données sur les employés (p. ex. noms, adresses, informations sur les salaires);
- les données relatives à votre avantage concurrentiel (p. ex. prix et marges de profit).

Les données des clients et les données sensibles peuvent être enregistrées dans des bases de données en ligne ou sur vos dispositifs de sauvegarde. Veillez à ce que ces données sensibles soient cryptées et sécurisées par un mot de passe fort, quel que soit l'endroit où elles sont stockées. Si vous utilisez un service d'hébergement Web ou une plateforme de commerce électronique, choisissez le niveau de sécurité le plus élevé possible.

Utiliser une plateforme de commerce électronique sécurisée

Si vous vendez des marchandises en ligne ou si vous acceptez des paiements en ligne, il est probable que vous utilisiez une plateforme de commerce électronique. Plusieurs plateformes de commerce électronique intègrent des solutions de cybersécurité qui peuvent protéger votre entreprise contre les cybermenaces.

Si vous êtes à la recherche d'une nouvelle plateforme de commerce électronique, renseignez-vous sur les différentes caractéristiques et options de sécurité proposées. Il peut s'agir d'éléments tels que l'authentification multifactorielle (AMF), le cryptage des données des clients, les alertes aux menaces en temps réel et les fonctions de conformité.

Si vous disposez déjà d'une plateforme de commerce électronique, veillez à réévaluer les fonctionnalités offertes.

Comme toujours, assurez-vous de mettre à jour les logiciels que vous utilisez. Les logiciels obsolètes peuvent présenter des failles de sécurité susceptibles de donner accès aux cybercriminels à votre boutique en ligne.

ACTIVER LES MISES À JOUR AUTOMATIQUES

Pour protéger vos appareils contre les cybermenaces, mettez régulièrement à jour les systèmes d'exploitation et les applications de vos appareils et installez les correctifs de sécurité. En plus de corriger des bogues, d'améliorer la convivialité et le rendement, les mises à jours et les correctifs contiennent souvent des éléments très importants pour la protection de la sécurité de votre entreprise, notamment des améliorations qui tiennent compte des plus récents virus et cyberattaques. Si vous ne mettez pas régulièrement à jour votre système d'exploitation et vos logiciels, les cybercriminels pourront utiliser ces vulnérabilités pour compromettre vos appareils, vos comptes et vos données.

Vous pouvez activer les mises à jour automatiques de vos appareils et logiciels ou les programmer à un moment où les systèmes ne sont pas utilisés de manière aussi active, par exemple la nuit. Si les mises à jour automatiques ne sont pas disponibles, installez-les dès que vous y êtes invité.



[Retour à la table des matières](#)

ÉLABORER UN PLAN DE CYBERSÉCURITÉ

Toute entreprise devrait disposer d'un plan de cybersécurité. Ce plan devrait comporter des procédures détaillées pour les opérations quotidiennes et, idéalement, un plan d'intervention en cas d'incident (voir **l'étape 9 pour l'établissement d'un plan d'intervention en cas d'incident**).

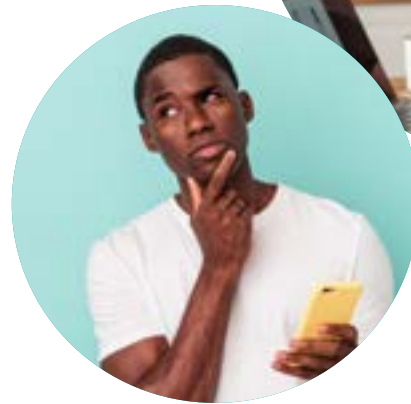
Si votre entreprise dispose d'un plan sur la manière de gérer adéquatement la cybersécurité, vos activités seront beaucoup plus sécuritaires.

Un plan de cybersécurité définit les règles que les employés d'une entreprise doivent respecter. Il doit comprendre des informations sur les logiciels qu'ils sont autorisés à télécharger, la manière de repérer un courriel d'hameçonnage et les rôles et responsabilités de chacun en ce qui concerne les renseignements commerciaux qu'ils peuvent partager en ligne.

Un plan de cybersécurité vous permettra, ainsi qu'à vos employés, de contribuer à la cybersécurité de votre entreprise. Il guidera les employés lorsqu'ils auront des questions ou des inquiétudes concernant la cybersécurité.

Le plan de cybersécurité doit tenir compte des plus récentes menaces et informations en matière de cybersécurité.

Les politiques de cybersécurité doivent être adaptées à chaque entreprise. Cela dit, il y aura probablement des éléments communs à ces politiques, tels que la sécurité relative à l'utilisation d'Internet, du courrier électronique et des médias sociaux.



Les entreprises canadiennes sont plus prudentes en matière de cybersécurité

En 2021, 26 % des entreprises canadiennes avaient mis en place des politiques écrites relatives à la cybersécurité, soit une augmentation d'au moins 4 % depuis 2019.

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



Retour à la table des matières

Établir une politique d'utilisation d'Internet

Une politique d'utilisation d'Internet fournit des informations importantes sur ce que les employés peuvent faire en ligne en utilisant les appareils de l'entreprise. Dans la plupart des cas, ces informations comprennent :

- des restrictions sur les types de sites Web que les employés sont autorisés à visiter;
- des lignes directrices sur les types de logiciels qu'ils peuvent télécharger, ainsi que les conditions à remplir pour obtenir l'autorisation de télécharger de nouveaux programmes;
- une obligation d'utiliser des phrases de passe ou des mots de passe complexes pour tous les appareils et comptes;
- des attentes en matière de mises à jour logicielles.

Établir des règles de sécurité pour l'utilisation du courrier électronique et de la messagerie

De nombreux cybercriminels utilisent le courrier électronique et la messagerie comme tactique clé pour voler des informations à leurs victimes. Certaines règles et mesures de sensibilisation devraient inclure :

- recommander aux employés de se méfier de l'ouverture et de la réponse à des courriels et messages directs suspects;
- demander aux employés d'éviter d'ouvrir les pièces jointes, à moins qu'elles ne proviennent de personnes et d'organisations de confiance;
- limiter le nombre de courriels personnels envoyés à partir des comptes professionnels des employés et ainsi limiter l'exposition de l'entreprise aux menaces en ligne provenant de contacts personnels;
- préciser quand il est approprié pour les employés de partager leur adresse courriel professionnelle (limité aux personnes et aux organisations de confiance);
- mentionner à vos employés d'éviter d'utiliser le symbole « @ », mais plutôt le formatage tel que « john à entrepriseX point com » afin que les polluposteurs ne puissent pas extraire l'adresse électronique.

7. Élaborer un plan de cybersécurité

Établir une politique en matière de médias sociaux

Les médias sociaux ne sont plus facultatifs pour la plupart des entreprises : ils sont essentiels. Les entreprises sont donc plus que jamais vulnérables aux menaces que les cybercriminels font peser sur elles par l'intermédiaire des médias sociaux. Voici quelques conseils pour mettre en place une politique relative aux médias sociaux :

- fixer des règles concernant les informations professionnelles qui peuvent être partagées en ligne et l'endroit où elles peuvent l'être;
- interdire aux employés de publier des informations confidentielles et exclusives;
- créer des directives pour que les employés puissent savoir s'ils peuvent utiliser leur adresse courriel professionnelle pour s'inscrire à des sites de médias sociaux et à des infolettres;
- établir des lignes directrices quant au bon usage des marques de commerce de l'entreprise.

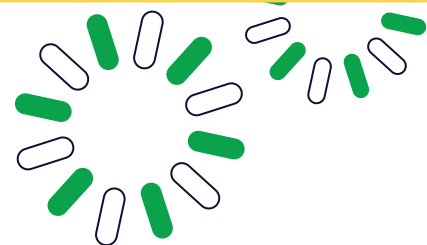
Établir un plan de télétravail et une politique « Prenez vos appareils personnels (PAP) »

Décidez comment (et si) les employés peuvent accéder aux données professionnelles sur leurs appareils personnels et quelle est la procédure à suivre en cas de perte ou de vol d'un appareil. Si un employé quitte l'entreprise, veillez à lui retirer l'accès à vos comptes.



Modèle

Vous trouverez un modèle de plan de cybersécurité **à la fin de ce guide.**



Retour à la table des matières

FORMER LES EMPLOYÉS

La cybersécurité est l'affaire de tous. L'erreur d'un seul employé pourrait causer la propagation d'un virus d'un appareil professionnel à tout le système de l'organisation. Il est important de faire de la cybersécurité un élément fondamental de votre entreprise afin que les employés comprennent l'incidence qu'ils ont sur la cybersécurité d'un point de vue personnel et professionnel.

Faire part du plan de cybersécurité de votre entreprise

En faisant savoir aux employés ce qui est cybersécuritaire et ce qui ne l'est pas, vous pouvez les sensibiliser à la manière dont ils peuvent protéger votre entreprise contre les cybermenaces. Faites part de votre plan de cybersécurité à vos employés et expliquez-leur les raisons de sa mise en place. Un personnel bien informé peut ainsi mieux se défendre contre les cyberincidents, puisque les cybercriminels s'appuient souvent sur les vulnérabilités liées à l'erreur humaine.

La cybersécurité se traduit par des actions individuelles, comme demeurer vigilant et se méfier des tentatives de fraude. Les tentatives de fraude, telles que l'hameçonnage ou **le harponnage**, ciblent souvent spécifiquement les entreprises. Tous les membres de votre entreprise doivent connaître les **signaux d'alarme** à surveiller et suivre le plan de sécurité de votre entreprise en matière de courrier électronique et de messagerie.

L'intégration des nouveaux employés doit également comprendre une présentation du plan de cybersécurité de l'entreprise.



Sensibilisation et formation

Élaborez des programmes de formation et de sensibilisation à la cybersécurité à l'intention de vos employés et employées et créez des défis ou des activités auxquels tout le monde participe. Par exemple, voyez quel département peut signaler le plus grand nombre de courriers électroniques frauduleux en un mois. Lorsque les employés s'engagent activement et avec diligence dans leur cybersécurité personnelle, cela se répercute sur la sécurité globale de l'entreprise.

Partagez les informations sur les nouvelles menaces dès que vous en avez connaissance et encouragez vos employés à vous signaler, ainsi qu'à la direction ou à l'équipe informatique, toute information suspecte. Une fois que vous avez mis en place un plan d'intervention en cas d'incident (voir **l'étape 9**), faites passer à vos employés un test de réponse aux incidents afin de vous familiariser avec le plan et de vous assurer que chaque membre comprend son rôle dans la récupération.

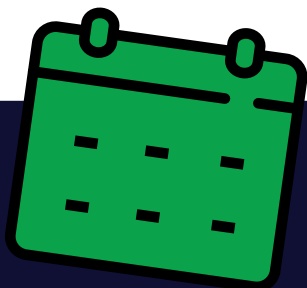


Retour à la table des matières

Cours de formation à la cybersécurité pour les petites entreprises

Le Carrefour de l'apprentissage du Centre pour la cybersécurité propose un cours en ligne gratuit et autodidacte pour tous ceux qui souhaitent améliorer la position de leur organisation en matière de cybersécurité.

Le cours 625 : Cybersécurité pour les petites et moyennes entreprises, est conçu pour les apprenants ayant des connaissances techniques minimales et vous aidera à protéger votre entreprise en vous expliquant comment mettre en œuvre des pratiques et des contrôles essentiels en matière de cybersécurité.



Mois de la sensibilisation à la cybersécurité

Octobre est le Mois de la sensibilisation à la cybersécurité (Mois de la cybersécurité) et une bonne occasion de parler de la cybersécurité et d'organiser des séances de formation.

Visitez le site [PensezCybersecurite.ca/](https://www.PensezCybersecurite.ca/) **MoisDeLaCybersecurite** pour obtenir du matériel que vous pouvez utiliser pour promouvoir la cybersécurité dans votre entreprise.



Retour à la table des matières

ÉTABLIR UN PLAN D'INTERVENTION EN CAS D'INCIDENT



Même si vous faites tout ce qu'il faut pour assurer la cybersécurité de votre entreprise, celle-ci n'est jamais à l'abri d'un incident. Cependant, si vous vous préparez au pire, vous saurez quoi faire pour atténuer les risques.

Un plan d'intervention en cas de cyberincident comprend les processus et les procédures à suivre pour détecter, répondre et se remettre d'un cyberincident. Les étapes suivantes doivent être prises en compte lors de l'élaboration de votre plan d'intervention :

La détection

Dans la section « Détection » de votre plan d'intervention en cas de cyberincident, veuillez à inclure des détails sur les points suivants :

- identifier qui et quels systèmes surveillent les appareils et les données;
- déterminer comment et à qui les employés doivent signaler un problème ou une préoccupation en matière de cybersécurité;
- identifier les partenaires internes et externes que vous aviserez en cas d'incident (par exemple, les fournisseurs, les investisseurs);
- identifier les services professionnels dignes de confiance auxquels vous pourriez faire appel pour vous aider à résoudre le cyberincident;
- déterminer comment vous pourriez parler publiquement de l'incident afin de préserver la réputation de votre entreprise et d'aviser les utilisateurs de pannes potentielles.

La réponse

Dans la section « Réponse » de votre plan d'intervention en cas de cyberincident, veuillez à inclure des détails sur les points suivants :

- déconnecter tous les appareils de votre réseau dès que possible (se référer à la liste d'inventaire des biens créée à **l'étape 1**);
- suspendre temporairement l'accès des employés afin de détecter et d'arrêter d'autres intrusions;
- faire appel à des services professionnels pour résoudre le problème, au besoin;
- changer tous les mots de passe concernés et activer l'authentification multifactorielle (AMF);
- changer les mots de passe qui ont pu être compromis par l'attaque, en particulier ceux des comptes administratifs;
- contacter votre institution financière si des informations financières ont été impliquées;
- signaler les détails de l'attaque au poste de police de votre région;
- signaler l'attaque au Centre antifraude du Canada et au Centre canadien pour la cybersécurité pour aider à protéger votre entreprise et d'autres entreprises contre une éventuelle attaque similaire.



Retour à la table des matières

La récupération

Dans la section « Récupération » de votre plan d'intervention en cas de cyberincident, veillez à inclure des détails sur les points suivants :

- restaurer vos systèmes à partir d'une sauvegarde;
- mettre à jour tous les logiciels, y compris les logiciels antivirus, les pare-feu et les micrologiciels, une fois que les systèmes sont opérationnels;
- exécuter les logiciels antimaliciel et antivirus sur tous les systèmes et appareils connectés;
- effectuer les correctifs et les mises à jour des appareils en cas de vulnérabilité;
- identifier les failles dans votre approche de la cybersécurité qui ont mené à l'attaque.



Pour plus de détails sur l'établissement d'un plan d'intervention en cas de cyberincident, consultez la publication du Centre canadien pour la cybersécurité : **Élaborer un plan d'intervention en cas d'incident (ITSAP.40.003)**.

Modèle

Vous pouvez trouver un modèle de plan d'intervention en cas de cyberincident **à la fin de ce guide**.



Tester votre plan

Nous vous recommandons de tester votre plan d'intervention. Cela vous permettra de déterminer les incohérences et d'aborder les aspects de votre plan qui nécessitent une amélioration. Voici quatre approches différentes pour tester votre plan d'intervention :

- Dresser une liste de vérification** : relisez et expliquez chaque étape du plan d'intervention. Énumérez tous les biens et systèmes qui doivent être pris en compte en cas de cyberattaque.
- Revoir la procédure pas à pas** : passez en revue les étapes des différents éléments du plan d'intervention afin de déceler les lacunes lors de l'examen spécifique d'un incident ou d'une catastrophe.
- Faire une simulation** : faites une simulation du plan d'intervention à l'aide d'un incident fictif. Les tests de simulation permettront à votre équipe de se familiariser avec ses rôles et ses responsabilités et d'évaluer le bon fonctionnement du plan d'intervention.
- Tester les systèmes** : mettez en place et testez les systèmes de sauvegarde pour confirmer s'ils peuvent effectuer les opérations adéquatement et soutenir les processus clés. Testez vos systèmes de sauvegarde en déconnectant partiellement et totalement vos systèmes principaux afin de vous assurer que les processus opérationnels peuvent se poursuivre si les systèmes sont compromis.

Tester vos systèmes permet d'évaluer les limites que vous pourriez rencontrer lors d'une cyberattaque. Il est important de tester la manière dont vos systèmes peuvent soutenir au mieux vos opérations lorsque des incidents se produisent, afin d'assurer un processus de récupération sans heurts.



Retour à la table des matières

SE TENIR AU FAIT EN MATIÈRE DE CYBERSÉCURITÉ

Le contexte des cybermenaces évolue constamment avec la découverte de nouvelles vulnérabilités et de nouvelles tactiques de fraude.

Vous pouvez tenir votre organisation au fait des cybermenaces actuelles en suivant les nouvelles, les alertes et les ressources fournies par la campagne de sensibilisation du public de Pensez cybersécurité et du Centre canadien pour la cybersécurité.

- Suivez le Centre canadien pour la cybersécurité (**cybercentre_ca**) sur X pour connaître les dernières alertes et les derniers avis en matière de cybercriminalité.
- Visitez le site Web du Centre canadien pour la cybersécurité (**cyber.gc.ca**) pour obtenir des conseils d'experts, des services et un soutien en matière de cybersécurité pour les Canadiens.
- Visitez le site Web de Pensez cybersécurité (**Pensezcybersecurite.ca**) pour connaître les mesures simples que vous pouvez prendre pour vous protéger en ligne et les ressources nécessaires pour organiser le Mois de la sensibilisation à la cybersécurité au sein de votre organisation.
- Partagez vos connaissances et ces ressources avec vos fournisseurs et vos clients afin de sécuriser l'ensemble de votre chaîne d'approvisionnement.



Retour à la table des matières

CONCLUSION

Avec la multiplication des opérations commerciales en ligne, la cybersécurité est de plus en plus importante pour les petites entreprises. En mettant l'accent sur la cybersécurité dans toutes vos activités commerciales et en suivant les étapes décrites dans ce guide, vous pourrez aider votre entreprise à se défendre contre les cybermenaces de toutes sortes.

Pour en savoir plus et pour obtenir des modèles, visitez le site Pensezcybersecurite.ca/entreprises.



PLAN DE CYBERSÉCURITÉ

Nom de l'entreprise :



Ce plan de cybersécurité décrit la manière dont nous allons assurer la cybersécurité de notre entreprise. Il nous guidera chaque fois que nous aurons une question ou une inquiétude concernant la cybersécurité.

La dernière mise à jour de ce plan de cybersécurité a été effectuée le :	
La personne responsable de la cybersécurité au sein de est :	

Ces responsabilités incluent :

- consulter le guide de Pensez cybersécurité pour les petites entreprises;
- planifier, mettre en œuvre et conserver ce plan;
- aider les autres membres du personnel à comprendre les meilleures pratiques et politiques en matière de cybersécurité.

POLITIQUE CONCERNANT L'UTILISATION D'INTERNET

Le personnel de

- utilise des mots de passe complexes et active l'authentification multifactorielle (AMF) lorsque cela est possible;
- active les mises à jour automatiques ou installe les mises à jour dès qu'elles sont disponibles;
- demande l'autorisation avant de télécharger de nouveaux logiciels sur des appareils appartenant à l'entreprise;
- n'utilise pas les appareils appartenant à l'entreprise pour commettre toute activité illégale, y compris le piratage de musique, de films et d'autres contenus.





SÉCURITÉ DU COURRIER ÉLECTRONIQUE ET DE LA MESSAGERIE

Le personnel de

- connaît les **7 signaux de l'hameçonnage**;
- est prudent lorsqu'ils ouvrent des courriels et des messages suspects;
- n'ouvre pas les pièces jointes suspectes;
- signale toute activité suspecte à
- ne partage leur adresse électronique professionnelle qu'avec des personnes et des organisations en qui il a confiance;
- évite d'utiliser le symbole « @ » lors de la publication en ligne de l'adresse électronique de l'entreprise – il utilise plutôt un formatage tel que « jean a commercial entreprisesxyz point com ».

POLITIQUE CONCERNANT LES MÉDIAS SOCIAUX

Le personnel de

- utilise leur adresse électronique personnelle (et non celle de l'entreprise) pour s'inscrire à des comptes de médias sociaux personnels et à des infolettres;
- ne partage pas de renseignements confidentiels ou sensibles sur les médias sociaux;
- demande l'autorisation avant de publier ou de répondre sur les médias sociaux au nom de






PLAN APORTEZ VOTRE APPAREIL

Le personnel de _____ qui utilise leurs propres appareils pour les besoins de l'entreprise :

- doit maintenir leur appareil personnel à jour avec un système d'exploitation récent et activer les mises à jour automatiques;
- ne peut pas utiliser un appareil personnel qui a été piraté (iOS), rooté (Android) ou compromis de toute autre manière;
- ne peut télécharger des applications qu'à partir de sources fiables telles que la boutique d'applications de l'appareil;
- doit régler leur appareil pour qu'il se verrouille automatiquement et se déverrouille à l'aide d'un code NIP, d'un mot de passe ou d'un code biométrique;
- ne doit pas accéder aux informations sensibles de l'entreprise en utilisant leur appareil personnel;
- doit savoir qui contacter (et avoir les bonnes coordonnées) en cas de problèmes de sécurité ou de perte ou de vol de leurs appareils;
- doit effacer toutes les informations personnelles et celles de l'entreprise avant de retourner ou de mettre au rebut un appareil personnel.

PLAN DE DÉPART DES EMPLOYÉ.E.S

Lorsqu'un-e employé-e quitte

- les biens professionnels tels que les ordinateurs portables, les clés et les badges d'accès doivent être restitués rapidement;
 - l'accès aux comptes de l'entreprise doit être supprimé.
- 

PLAN D'INTERVENTION EN CAS D'INCIDENT

Un plan d'intervention en cas d'incident comprend les processus et les procédures à suivre pour détecter un cyberincident, y répondre et assurer la récupération.



DÉTECTION

La personne responsable de la cybersécurité est chargée de surveiller les systèmes et les données de l'entreprise afin de détecter les cyberincidents.

Le personnel doit signaler tout problème ou préoccupation de sécurité à la personne responsable de la cybersécurité.

La personne responsable de la cybersécurité chez est :	Nom : Coordonnées : Autres coordonnées :
--	---

PERSONNES-RESSOURCES :

En cas de cyberincident au sein de _____, la personne responsable de la cybersécurité informera :

la personne responsable de la communication chez	Nom : Coordonnées :
---	--

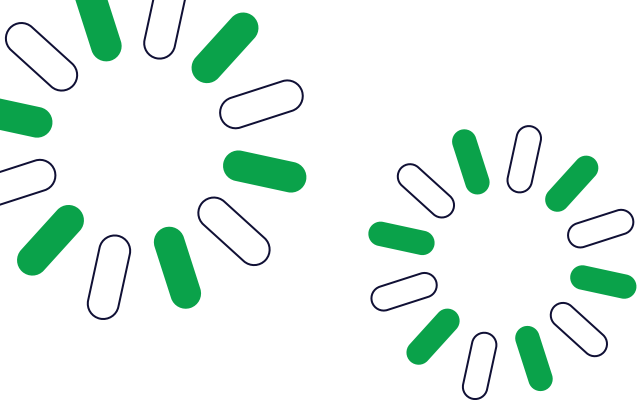
En fonction des détails de l'incident, la personne responsable de la cybersécurité informera également :

la personne responsable des affaires juridiques chez	Nom : Coordonnées :
les principaux fournisseurs de	Nom : Coordonnées :
les principaux clients de	Nom : Coordonnées :
les investisseurs au sein de	Nom : Coordonnées :

En fonction de la gravité de l'incident, la personne responsable de la cybersécurité fera appel à un fournisseur de services informatiques professionnels :

Nom du fournisseur : Coordonnées :

Déterminez comment vous pourriez communiquer publiquement des informations sur l'incident afin de préserver la réputation de votre entreprise et d'informer les utilisateurs des pannes potentielles.



RÉPONSE

Voici les mesures à prendre pour répondre à un cyberincident :

- 1** Déconnecter tous les appareils du réseau dès que possible (se reporter à la liste d'inventaire des biens).
- 2** Suspendre temporairement l'accès des employés afin de détecter et d'empêcher d'autres intrusions.
- 3** Faire appel à des services professionnels pour résoudre le problème, si nécessaire.
- 4** Modifier tous les mots de passe concernés et activer l'authentification multifactorielle (AMF).
- 5** Modifier les autres mots de passe susceptibles d'avoir été compromis par l'attaque, en particulier ceux des comptes administratifs.
- 6** Communiquer publiquement l'incident par une déclaration telle que :

Nous avons connu un incident de cybersécurité [plus tôt dans la journée] et nous travaillons [avec des experts en cybersécurité] pour résoudre la situation. Nous nous excusons sincèrement auprès de notre précieuse clientèle pour les désagréments causés. Notre priorité est de résoudre ce problème [et de fournir des informations aux personnes concernées] dès que possible.
- 7** Contacter son institution financière si des données financières sont impliquées.
- 8** Signaler les détails de l'attaque au service de police de sa région.
- 9** Signaler l'attaque au **Centre antifraude du Canada** et au **Centre canadien pour la cybersécurité** pour aider à protéger l'entreprise et d'autres entreprises contre une attaque similaire potentielle.

RÉCUPÉRATION

Voici les mesures à prendre pour assurer la récupération à la suite d'un cyberincident :

- 1** Restaurer les systèmes à partir de la dernière sauvegarde.
- 2** Mettre à jour tous les logiciels, y compris le logiciel antivirus, le pare-feu et le micrologiciel une fois que les systèmes sont opérationnels.
- 3** Exécuter un logiciel antimaliciel et antivirus sur tous les systèmes et appareils connectés.
- 4** Mettre à jour les appareils.
- 5** Identifier les failles dans l'approche de la cybersécurité qui ont conduit à l'incident.

