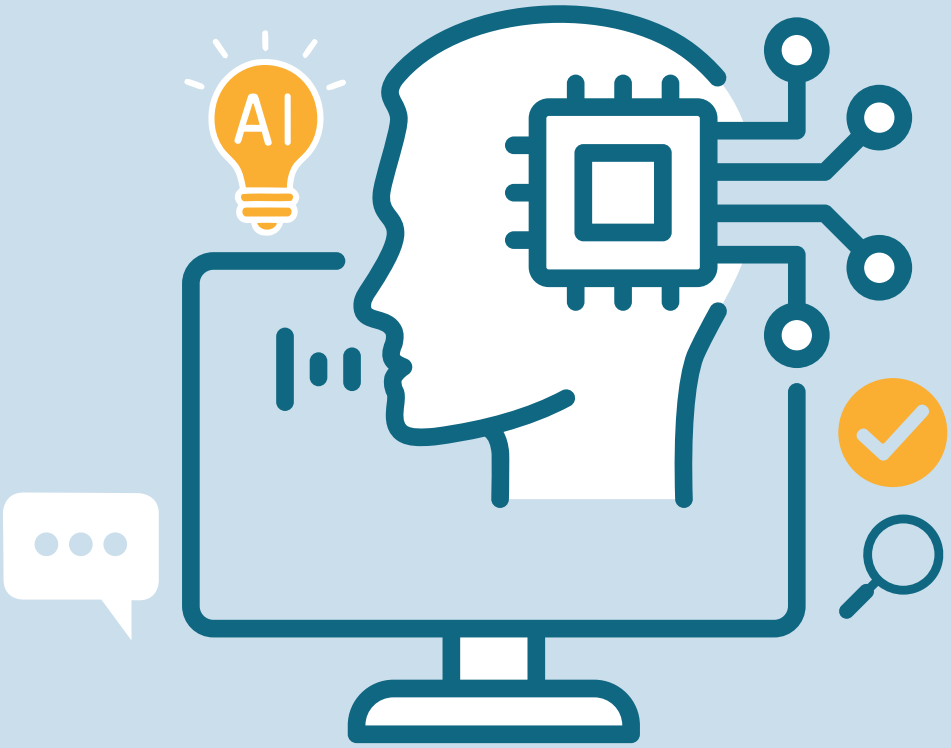
Protection de la vie privée numérique et cybersécurité pour les petits centres



AMSSA
Strengthening Diversity In BC

Introduction : Pourquoi la protection de la vie privée et la cybersécurité sont importantes

Objectif

Ce guide est conçu pour aider les petits organismes d'établissement à renforcer leurs pratiques en matière de protection de la vie privée et de cybersécurité de façon pratique et accessible. Il met l'accent sur la protection des renseignements sensibles des clients, des données du personnel et des systèmes organisationnels, tout en reconnaissant que de nombreuses petites équipes disposent de ressources techniques limitées ou n'ont pas de soutien informatique dédié.

Pourquoi c'est important

Les organismes d'établissement travaillent souvent avec des renseignements très sensibles, tels que des documents d'immigration, des pièces d'identité, des coordonnées personnelles et des notes de dossiers. La protection de ces renseignements est essentielle pour maintenir la confiance des clients et des partenaires.

Les incidents de cybersécurité peuvent perturber les services, nuire à la réputation de l'organisme et entraîner des risques juridiques ou réglementaires si des renseignements personnels sont exposés.

À mesure que les organismes adoptent davantage d'outils numériques pour la communication, le stockage de fichiers et la prestation de services, la protection des comptes, des appareils et des données devient un élément essentiel d'une prestation de services responsable.

Pourquoi c'est réalisable

Beaucoup de personnes pensent que la cybersécurité nécessite une expertise technique complexe, alors que les protections les plus efficaces reposent souvent sur des pratiques simples et des habitudes quotidiennes que le personnel peut adopter.

Des actions comme l'utilisation de mots de passe forts, l'activation de l'authentification multifacteur, la reconnaissance des courriels suspects et la limitation de l'accès aux renseignements sensibles peuvent réduire considérablement les risques.

L'objectif n'est pas d'éliminer toutes les menaces possibles, mais de rendre votre organisme beaucoup plus difficile à cibler et mieux préparé à réagir si un incident survient.

Ce guide se concentre sur des mesures pratiques que les petites équipes peuvent mettre en œuvre, même sans personnel informatique, en utilisant des outils et des systèmes qu'elles possèdent déjà.

Comprendre les risques

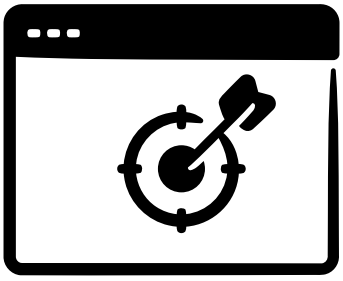
Risques cybernétiques courants

Les petits organismes font face à plusieurs des mêmes menaces que les grandes organisations, mais disposent souvent de moins de ressources pour les gérer.

- Courriels d'hameçonnage (phishing)
- Mots de passe faibles ou réutilisés
- Logiciels malveillants ou rançongiciels
- Partage imprudent de renseignements sensibles

Pourquoi les petits organismes sont ciblés

Les cybercriminels ciblent souvent les petits organismes parce qu'ils peuvent avoir moins de mesures de sécurité en place. Le personnel est souvent très occupé, multitâche et responsable de nombreuses tâches, ce qui peut permettre à des courriels ou demandes suspectes de passer inaperçus. Le manque de formation en cybersécurité peut également accroître les risques.



La réalité des incidents de cybersécurité

On croit souvent que les cyberattaques nécessitent des techniques de piratage sophistiquées. En réalité, la plupart des incidents commencent par des actions humaines simples, comme cliquer sur un lien malveillant, partager des identifiants de connexion ou utiliser des mots de passe faibles. La bonne nouvelle est que l'amélioration des pratiques quotidiennes peut prévenir de nombreux incidents de sécurité courants.

Pratiques simples de cybersécurité que chaque organisme devrait adopter

1 Utiliser l'authentification multifacteur (AMF)

L'authentification multifacteur ajoute une étape supplémentaire lors de la connexion, comme un code envoyé à votre téléphone. Même si un mot de passe est compromis, l'AMF peut aider à empêcher l'accès non autorisé.

2 Avoir une bonne politique de mot de passe

Des mots de passe forts et uniques aident à prévenir l'accès non autorisé aux comptes. Évitez de réutiliser les mêmes mots de passe et envisagez l'utilisation d'un gestionnaire de mots de passe sécurisé.

3 Maintenir les systèmes à jour

Les mises à jour régulières corrigent des vulnérabilités de sécurité que les attaquants peuvent exploiter. Activez les mises à jour automatiques sur les ordinateurs, les téléphones et les logiciels lorsque c'est possible.

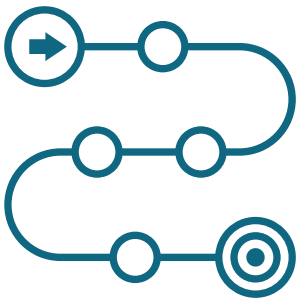
4 Offrir une formation au personnel

La formation aide le personnel à reconnaître les menaces courantes, comme l'hameçonnage et les liens suspects. Même de courts rappels peuvent réduire considérablement le risque d'incidents de sécurité accidentels.

Conseils pratiques en cybersécurité

- Verrouiller votre ordinateur lorsque vous vous absentez de votre poste
- Vérifier les adresses des destinataires avant d'envoyer des renseignements sensibles
- Stocker les fichiers dans des systèmes approuvés, et non sur des appareils personnels ou des clés USB
- Signaler immédiatement les appareils perdus ou toute activité suspecte
- Avoir un plan de réponse aux incidents de sécurité
- Utiliser des réseaux Wi-Fi distincts pour le personnel et pour les invités ou clients
- Avoir une politique informatique écrite et offrir une formation sur les procédures et normes

Créer un processus de sécurité simple



Pourquoi c’est important

Même les petits organismes bénéficient de procédures claires et simples. Lorsque le personnel sait quoi faire en cas de problème, les incidents de sécurité peuvent être traités plus rapidement et avec moins de confusion. La mise en place de quelques processus de base aide à protéger les renseignements des clients et garantit une réponse cohérente du personnel face aux situations courantes.

Réponse aux incidents

Le personnel devrait comprendre les étapes à suivre lorsqu’une situation suspecte se produit. Cela comprend savoir qui aviser en cas d’activité inhabituelle, comment signaler la perte ou le vol d’appareils, et quoi faire si un compte peut avoir été compromis. Des procédures de signalement claires aident l’organisme à réagir rapidement et à limiter les dommages potentiels.

Accueil et départ du personnel

La gestion des accès aux systèmes lors de l’arrivée ou du départ du personnel est essentielle à la protection de l’information. Les nouveaux employés ne devraient avoir accès qu’aux systèmes nécessaires à leur rôle. Lorsqu’un employé quitte l’organisme, ses accès doivent être retirés immédiatement.

Accès des fournisseurs et partenaires

Les fournisseurs externes ou partenaires peuvent parfois nécessiter un accès temporaire aux systèmes. Cet accès doit être limité à ce qui est strictement nécessaire et retiré une fois le travail terminé. Cela aide à réduire le risque d’exposition inutile de renseignements sensibles.

Votre politique informatique

Tout organisme qui traite des renseignements sur les clients devrait avoir une politique informatique claire. Une politique TI aide le personnel à comprendre comment la technologie doit être utilisée, comment l'information doit être protégée et quoi faire lorsqu'un problème survient. Elle n'a pas besoin d'être complexe ou technique, mais elle doit être documentée, expliquée au personnel et appliquée de façon cohérente.

Éléments à inclure

Utilisation acceptable de la technologie

Définit comment le personnel peut utiliser les ordinateurs, les réseaux, le courriel et l'accès Internet de l'organisme à des fins professionnelles.

Contrôle des accès

Précise comment l'accès aux systèmes et à l'information est accordé, révisé et retiré.

Sécurité des appareils

Établit les attentes en matière de sécurisation des ordinateurs portables, des téléphones mobiles et des autres appareils utilisés pour le travail.

Gestion des changements

Assure que les changements importants apportés aux systèmes, aux logiciels ou à l'infrastructure sont examinés et documentés.

Signalement et réponse aux incidents

Explique comment le personnel doit signaler les préoccupations en matière de sécurité, la perte d'appareils ou les atteintes présumées à la sécurité.

Accès des fournisseurs et des tiers

Établit des règles pour accorder l'accès aux fournisseurs de services et aux partenaires externes.

Mots de passe et authentification

Établit des règles concernant les mots de passe forts, la protection des comptes et l'utilisation de l'authentification multifacteur.

Protection des données et vie privée

Décrit comment les renseignements sensibles des clients et de l'organisme doivent être stockés, partagés et protégés.

Logiciels et applications approuvés

Définit quels logiciels et services infonuagiques sont approuvés pour une utilisation organisationnelle.

Courriels et communications

Fournit des indications pour reconnaître les messages suspects et manipuler de façon sécuritaire les pièces jointes et les liens.

Sauvegarde et récupération des données

Définit comment les données importantes sont sauvegardées et comment les systèmes peuvent être rétablis après une panne ou une attaque.

Télétravail et accès au réseau

Précise les attentes concernant l'accès sécuritaire aux systèmes de l'organisme à partir du domicile ou de réseaux publics.

Ressources supplémentaires

Canadian Centre for Cyber Security
Fournit des conseils pratiques, des alertes et des outils en cybersécurité pour les organisations de toutes tailles.
https://www.cyber.gc.ca

Office of the Privacy Commissioner of Canada
Offre des conseils sur les obligations en matière de protection de la vie privée et les meilleures pratiques pour protéger les renseignements personnels.
https://www.priv.gc.ca

BC Office of the Information and Privacy Commissioner
Met à disposition des ressources sur les responsabilités liées à la protection de la vie privée et à la gestion de l'information pour les organisations exerçant en Colombie-Britannique.
https://www.oipc.bc.ca/fr/

Get Cyber Safe
Programme de sensibilisation du gouvernement du Canada qui fournit des conseils simples pour rester en sécurité en ligne.
https://www.getcybersafe.gc.ca

National Cyber Threat Assessment
Présente un aperçu des menaces cybernétiques actuelles qui touchent les organisations canadiennes.
https://www.cyber.gc.ca/fr/orientation/evaluation-cybermenaces-nationales-2025-2026

Cyber101 - Free Cybersecurity Awareness Training
Propose des modules de formation courts et accessibles qui aident le personnel à reconnaître les menaces courantes et à améliorer la sensibilisation à la cybersécurité.
https://www.cyber101.com/fr/

Affiliation of Multicultural Societies and Service Agencies of British Columbia
Metrotower II, Suite 2308, 4720 Kingsway, Burnaby, British Columbia, V5H 4N2
1 888 355-5560 | 604 718-2780 | amssa@amssa.org | www.amssa.org