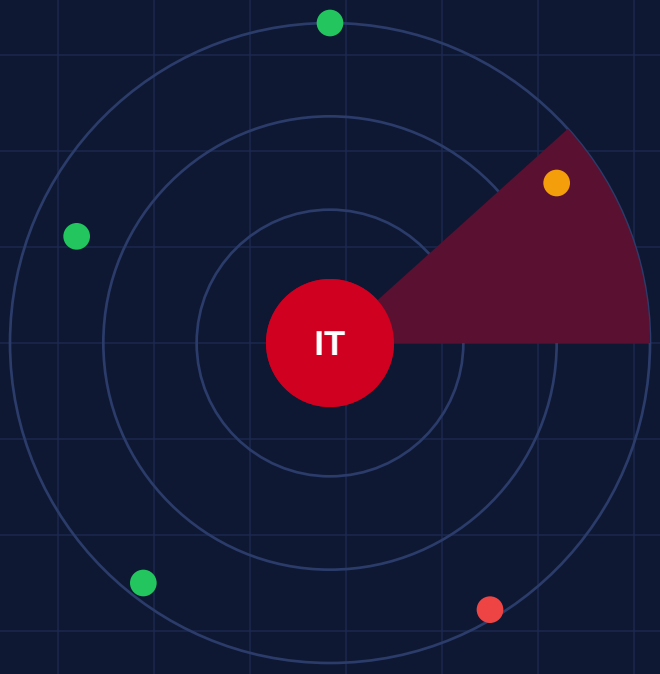
PING SYSTEMS · GUIDE GRATUIT

Le guide de cybersécurité pour petits bureaux

10 étapes concrètes pour protéger votre entreprise, votre informatique et les données de vos clients à l'ère de l'IA.



Ping Systems Inc.

Édition de novembre 2026 · Pour les petits bureaux d'Ottawa, de Gatineau et d'ailleurs

pingsystems.ca · 613-510-1264 · info@pingsystems.ca

Pourquoi maintenant

L’intelligence artificielle a changé la vitesse des cyberattaques. Les outils qui aident les éditeurs à trouver et corriger les failles aident aussi les criminels à repérer les points faibles, à rédiger des arnaques convaincantes et à imiter des voix.

Les bases d’une bonne défense n’ont pas changé. Ce qui a changé, c’est le peu de temps dont vous disposez pour les mettre en place.

1 sur 6

C’est la part des entreprises canadiennes touchées par un incident de cybersécurité en 2025.

Statistique Canada, octobre 2026

0 jour

Délai médian entre la publication d’une faille et les premières attaques en 2026, contre 771 jours en 2018.

ESET, d’après le Zero Day Clock, septembre 2026

10 000+

Failles de gravité élevée ou critique trouvées en un mois par des partenaires utilisant un seul modèle d’IA.

Anthropic, Project Glasswing, mai 2026

Comment utiliser ce guide

Suivez les dix étapes dans l’ordre. Chaque étape comporte une courte liste de contrôle. Cochez ce qui est déjà en place, à l’écran ou sur papier, puis comblez les manques en commençant par les étapes 1 à 3. En cas de doute, considérez que ce n’est pas fait. Le tableau de la page 9 donne une vue d’ensemble rapide.

ÉTAPE 01

1 Appliquer les mises à jour vite et automatiquement

POURQUOI C'EST IMPORTANT

La plupart des attaques exploitent encore des failles connues. Dès qu'un correctif sort, les attaquants l'étudient, souvent en quelques heures. Chaque jour d'attente laisse la porte ouverte.

LISTE DE CONTRÔLE

- ☐ Activez les mises à jour automatiques de Windows, macOS, des navigateurs et des applications bureautiques.
- ☐ Mettez aussi à jour pare-feu, routeurs, bornes Wi-Fi et imprimantes, souvent oubliés.
- ☐ Appliquez les mises à jour de sécurité critiques en quelques jours, pas en quelques semaines.
- ☐ Vérifiez chaque mois que chaque appareil a bien installé ses mises à jour.

ÉTAPE 02

2 Activer l'authentification multifacteur partout

POURQUOI C'EST IMPORTANT

Les mots de passe volés sont l'une des portes d'entrée les plus courantes. Une deuxième vérification bloque la plupart de ces attaques, même si le mot de passe est connu.

LISTE DE CONTRÔLE

- ☐ Activez la MFA sur la messagerie, Microsoft 365 ou Google Workspace, la banque, le logiciel comptable et l'accès à distance.
- ☐ Préférez une application d'authentification, les clés d'accès (passkeys) ou les clés de sécurité aux SMS.
- ☐ Utilisez une MFA résistante à l'hameçonnage, comme les clés d'accès ou de sécurité, pour les comptes administrateurs.
- ☐ N'approuvez jamais une demande de connexion que vous n'avez pas lancée vous-même.

3

ÉTAPE 03

Sauvegarder, et prouver que la restauration fonctionne

POURQUOI C'EST IMPORTANT

De bonnes sauvegardes transforment un rançongiciel en simple contretemps. Des sauvegardes jamais testées échouent souvent le jour où vous en avez besoin.

LISTE DE CONTRÔLE

- ☐ Conservez trois copies des données importantes, sur deux types de supports, dont une hors ligne ou non modifiable.
- ☐ Sauvegardez aussi le cloud, y compris les e-mails et fichiers Microsoft 365 ou Google Workspace.
- ☐ Testez une restauration au moins tous les trois mois et notez le temps nécessaire.
- ☐ Protégez les systèmes de sauvegarde par un mot de passe robuste qui leur est propre et la MFA.

4

ÉTAPE 04

Réduire ce qui est exposé sur Internet

POURQUOI C'EST IMPORTANT

Les criminels balaient Internet en permanence à la recherche de portes ouvertes : bureau à distance, anciens VPN, pages d'administration.

LISTE DE CONTRÔLE

- ☐ N'exposez jamais le bureau à distance (RDP) directement sur Internet. Utilisez un VPN ou un service d'accès à distance sécurisé avec MFA.
- ☐ Fermez les ports et services inutilisés, et changez tous les mots de passe administrateur par défaut.
- ☐ Tenez à jour le micrologiciel des pare-feu et des VPN, cibles fréquentes des attaquants.
- ☐ Listez chaque service exposé en ligne et revoyez cette liste deux fois par an.

ÉTAPE 05

5 Connaître son parc, et retirer ce qui n’est plus pris en charge

POURQUOI C’EST IMPORTANT

On ne protège pas un appareil ou un compte dont on ignore l’existence. Un système qui ne reçoit plus de mises à jour de sécurité reste vulnérable pour de bon.

LISTE DE CONTRÔLE

- ☐ Tenez une liste simple des ordinateurs, téléphones, serveurs, équipements réseau, logiciels et services cloud.
- ☐ Remplacez ou isolez tout ce qui ne reçoit plus de mises à jour de sécurité, comme les postes Windows 10 sans mises à jour étendues.
- ☐ Supprimez les logiciels et comptes inutilisés.
- ☐ Sachez qui, au bureau, est responsable de chaque système important.

ÉTAPE 06

6 Ne donner que les accès nécessaires

POURQUOI C’EST IMPORTANT

Quand un compte est piraté, les dégâts dépendent de ce à quoi il a accès.

LISTE DE CONTRÔLE

- ☐ N’utilisez pas de compte administrateur pour le travail quotidien.
- ☐ Retirez les accès le jour même du départ d’un employé.
- ☐ Vérifiez chaque trimestre qui peut ouvrir les dossiers partagés, les systèmes financiers et les dossiers clients.
- ☐ Utilisez des comptes distincts et protégés pour l’administration informatique.

ÉTAPE 07

7 Protéger les postes et la messagerie

POURQUOI C'EST IMPORTANT

La plupart des attaques arrivent par e-mail ou par un seul ordinateur compromis.

LISTE DE CONTRÔLE

- ☐ Utilisez une protection moderne des postes avec détection et réponse (EDR), surveillée par quelqu'un.
- ☐ Filtrez les e-mails entrants contre l'hameçonnage, les liens malveillants et les pièces jointes dangereuses.
- ☐ Configurez SPF, DKIM et DMARC pour empêcher les criminels d'envoyer facilement des e-mails en votre nom.
- ☐ Chiffrez portables et téléphones, et assurez-vous de pouvoir les effacer à distance en cas de perte.

ÉTAPE 08

8 Préparer l'équipe aux arnaques dopées à l'IA

POURQUOI C'EST IMPORTANT

L'IA rend crédibles les faux e-mails, SMS, appels et même vidéos. La fraude au détournement de paiement coûte chaque année des dizaines de millions de dollars aux entreprises canadiennes.

LISTE DE CONTRÔLE

- ☐ Confirmez toute demande de changement de coordonnées bancaires ou de virement en rappelant un numéro déjà connu, jamais celui du message.
- ☐ Convenez d'une vérification pour les demandes urgentes de la direction ou de l'informatique : rappel ou mot de code.
- ☐ Organisez une courte sensibilisation au moins deux fois par an, y compris aux faux appels du support informatique.
- ☐ Fixez des règles claires pour les outils d'IA : aucune donnée client ou personnelle dans un outil non approuvé par l'entreprise.

ÉTAPE 09

9 Surveiller, et s’assurer que quelqu’un réagit

POURQUOI C’EST IMPORTANT

Une attaque repérée tôt coûte moins cher et se contient plus facilement. Des journaux que personne ne lit ne protègent personne.

LISTE DE CONTRÔLE

- ☐ Centralisez les journaux de connexion et de sécurité de la messagerie, des postes et des pare-feu.
- ☐ Activez des alertes sur les connexions inhabituelles, les nouvelles règles de transfert d’e-mails et les modifications massives de fichiers.
- ☐ Désignez un responsable du suivi des alertes, y compris hors des heures de bureau pour les systèmes critiques.
- ☐ Séparez les systèmes clés pour qu’un problème ne puisse pas se propager facilement.

ÉTAPE 10

10 Tenir un plan d’incident d’une page

POURQUOI C’EST IMPORTANT

Dans la première heure d’un incident, un plan écrit à l’avance fait gagner du temps et de l’argent, et évite des erreurs coûteuses.

LISTE DE CONTRÔLE

- ☐ Notez qui appeler : votre prestataire informatique, votre banque, votre assureur et, si besoin, un avocat.
- ☐ Indiquez comment isoler un appareil infecté et où se trouvent vos sauvegardes.
- ☐ Connaissez vos obligations de déclaration pour les renseignements personnels (voir page 8).
- ☐ Répétez le plan une fois par an avec un court exercice sur table.

Si vous pensez avoir été piraté

Agissez vite, mais calmement. Ces étapes limitent les dégâts et préservent vos options.

1. **Ne payez pas et ne répondez pas à l’attaquant**
   Demandez conseil avant tout contact ou paiement.
2. **Isolez les appareils touchés**
   Débranchez le câble réseau ou coupez le Wi-Fi. Laissez l’appareil allumé : l’éteindre peut détruire des preuves utiles.
3. **Appelez votre prestataire informatique**
   Clients de Ping Systems : 613-510-1264.
4. **Appelez votre banque sans attendre si de l’argent a été transféré**
   Un signalement rapide augmente les chances de bloquer ou de récupérer un paiement.
5. **Changez les mots de passe depuis un appareil sain**
   Commencez par la messagerie et les comptes administrateurs.
6. **Signalez l’incident**
   Contactez votre police locale et le service Signaler la cybercriminalité et la fraude du Centre antifraude du Canada : antifraudcentre-centreantifraude.ca ou 1-888-495-8501. Vous pouvez aussi le signaler au Centre canadien pour la cybersécurité sur cyber.gc.ca.

Vos obligations en matière de vie privée

Partout au Canada (LPRPDE)
Si une atteinte aux renseignements personnels crée un risque réel de préjudice grave, déclarez-la au Commissariat à la protection de la vie privée du Canada et avisez les personnes concernées dès que possible. Conservez un registre de chaque atteinte pendant 24 mois, même mineure.

Au Québec, y compris à Gatineau (Loi 25)
Tenez un registre de tous les incidents de confidentialité. Si un incident présente un risque de préjudice sérieux, avisez avec diligence la Commission d’accès à l’information et les personnes concernées.

Renseignements de santé en Ontario
Les cliniques et autres dépositaires peuvent aussi avoir des obligations de notification au titre de la Loi sur la protection des renseignements personnels sur la santé (LPRPS) de l’Ontario.

Ces informations sont d’ordre général et ne constituent pas un avis juridique. Un avocat peut confirmer les règles applicables à votre organisation.

Tableau d’évaluation rapide

Évaluez chaque étape honnêtement. Une étape n’est en place que si tous les points de sa liste sont faits.

#		En place	En partie	Pas encore
1	Appliquer les mises à jour vite et automatiquement	☐	☐	☐
2	Activer l’authentification multifacteur partout	☐	☐	☐
3	Sauvegarder, et prouver que la restauration fonctionne	☐	☐	☐
4	Réduire ce qui est exposé sur Internet	☐	☐	☐
5	Connaître son parc, et retirer ce qui n’est plus pris en charge	☐	☐	☐
6	Ne donner que les accès nécessaires	☐	☐	☐
7	Protéger les postes et la messagerie	☐	☐	☐
8	Préparer l’équipe aux arnaques dopées à l’IA	☐	☐	☐
9	Surveiller, et s’assurer que quelqu’un réagit	☐	☐	☐
10	Tenir un plan d’incident d’une page	☐	☐	☐

8 à 10 en place
Une position solide. Continuez à tester les sauvegardes et à revoir les accès.

5 à 7 en place
Des manques réels subsistent. Corrigez d’abord les étapes 1 à 3, puis le reste.

0 à 4 en place
Risque élevé. Faites-vous aider dès maintenant : mises à jour, MFA et sauvegardes.

Comment Ping Systems vous aide

En tant que prestataire d’infogérance et de sécurité, nous mettons ces étapes en place et les maintenons dans la durée, pour que votre équipe se concentre sur ses clients.

- [ ] Mises à jour et surveillance des postes, serveurs et équipements réseau
- [ ] Déploiement de l’authentification multifacteur sur vos comptes
- [ ] Sauvegardes surveillées avec tests de restauration réguliers
- [ ] Gestion du pare-feu et accès à distance sécurisé
- [ ] Protection des postes et sécurité de la messagerie, y compris SPF, DKIM et DMARC
- [ ] Sensibilisation des équipes en langage simple
- [ ] Une équipe locale à Ottawa et à Gatineau, sur place si besoin

Plus de 20 ans d’expérience cumulée · En français ou en anglais · Des conseils clairs

Commencez par un audit informatique gratuit

Nous examinons vos postes, votre réseau, vos comptes, votre messagerie, vos sauvegardes et votre sécurité, puis vous remettons un plan écrit clair. Gratuit et sans engagement.

pingsystems.ca/fr/audit-informatique-gratuit
613-510-1264 · info@pingsystems.ca

Sources

1. Statistique Canada, Le Quotidien : environ une entreprise canadienne sur six touchée par des incidents de cybersécurité en 2025 (21 octobre 2026).
2. Centre canadien pour la cybersécurité : déclaration sur les modèles d’intelligence artificielle de pointe et leurs effets sur la cybersécurité (24 juin 2026).
3. Centre canadien pour la cybersécurité : Perspectives de la menace des rançongiciels 2025 à 2027 (janvier 2026).
4. Centre canadien pour la cybersécurité : Contrôles de cybersécurité de base pour les petites et moyennes organisations.
5. Centre canadien pour la cybersécurité : alerte AL26-028, campagne d’hameçonnage vocal visant les services d’assistance d’organisations canadiennes (28 octobre 2026).
6. Anthropic : Project Glasswing, an initial update (22 mai 2026).
7. SecurityBrief : AI shrinks exploit window to zero days, ESET warns (16 septembre 2026).
8. Centre antifraude du Canada : communiqué sur les pertes liées à la fraude par harponnage en 2025 (29 janvier 2026).
9. Commissariat à la protection de la vie privée du Canada : Ce que vous devez savoir au sujet de la déclaration obligatoire des atteintes aux mesures de sécurité.
10. Québec : Loi sur la protection des renseignements personnels dans le secteur privé, articles 3.5 à 3.8.

Ce guide est une information générale destinée à aider les petites organisations à réduire leur risque informatique. Il ne constitue pas un avis juridique, d’assurance ou professionnel, et aucune mesure ne supprime tout risque. Les chiffres proviennent des sources indiquées, aux dates de publication mentionnées. Ce PDF ne contient ni script, ni lien, ni fichier intégré. Ses cases à cocher sont la seule partie interactive et n’envoient rien. © 2026 Ping Systems Inc. Vous pouvez partager ce guide gratuitement, sans le modifier.