

OCTOBRE 2026 / GUIDE GRATUIT DE CINQ PAGES

Protégez-vous. Protégez votre entreprise.

Un guide pratique pour réduire les risques au quotidien, à la maison et au travail.



CINQ ESSENTIELS POUR COMMENCER

- ☐ Un mot de passe unique pour chaque compte important.
- ☐ L'authentification multifacteur (MFA) activée.
- ☐ Une vérification des demandes inattendues.
- ☐ Des mises à jour et une sauvegarde distincte.
- ☐ Un contact à joindre en cas de problème.

Utilisez les quatre pages suivantes comme liste de vérification. Choisissez une action, réalisez-la, puis passez à la suivante.

Protégez vos comptes.

Commencez par votre courriel principal : il sert souvent à rétablir l'accès à vos autres services.

01

Utiliser un gestionnaire de mots de passe

Attribuez à chaque compte un mot de passe unique ou une longue phrase de passe. Un gestionnaire fiable peut les créer et les conserver. Protégez-le avec une phrase de passe maîtresse robuste et la MFA. [1]

02

Ajouter une vérification de connexion

Activez la MFA partout où elle est offerte. Privilégiez les clés d'accès ou les clés de sécurité matérielles lorsqu'elles sont disponibles; elles peuvent résister à l'hameçonnage. Sinon, utilisez une méthode MFA prise en charge. N'approuvez aucune connexion que vous n'avez pas lancée. [2, 12]

03

Protéger les moyens de récupération

Vérifiez le courriel et le numéro de récupération. Conservez les codes de secours dans un endroit protégé, distinct de l'appareil de connexion. Ne communiquez ni mot de passe ni code de vérification à un appelant. [2, 10]

Faire une pause. Vérifier. Puis agir.

Une facture urgente, un lien de partage ou un nom familier peut cacher une fraude. Ouvrez l'application connue ou saisissez vous-même l'adresse officielle. Vérifiez les demandes inhabituelles par un moyen de contact déjà fiable. [3]

Exemple : « Nos coordonnées bancaires ont changé. Payez aujourd'hui. » Appelez le fournisseur au numéro déjà dans vos dossiers avant de modifier un paiement. Un message soigné ne prouve pas l'identité.

Sécurisez appareils et Wi-Fi.

Incluez ordinateurs, téléphones, navigateurs, applications et routeur.

01 Installer les mises à jour

Activez les mises à jour automatiques lorsque possible et effectuez les redémarrages requis. Passez par les réglages officiels plutôt que par une fenêtre surgissante. Remplacez ou mettez à niveau les logiciels sans correctifs de sécurité. [4]

02 Choisir des logiciels fiables

Installez les applications depuis les sources officielles. Gardez la protection intégrée et le pare-feu actifs. Pour un appareil professionnel, suivez les outils et les procédures approuvés par votre fournisseur TI. [6, 8]

03 Limiter les accès quotidiens

Verrouillez l'écran en votre absence. Utilisez si possible un compte standard au quotidien et réservez les droits administratifs aux changements approuvés. Demandez conseil sur le chiffrement et la conservation des clés de récupération. [6, 8]

04 Examiner le Wi-Fi

Changez les identifiants d'administration par défaut et utilisez un mot de passe Wi-Fi unique. Maintenez le micrologiciel à jour. Séparez les visiteurs et appareils connectés sur un réseau invité lorsque possible. [5]

STOP / VÉRIFIEZ

Un appel de « soutien » inattendu? N'installez pas d'outil de contrôle à distance à la demande d'un inconnu. Joignez votre fournisseur TI au numéro habituel. [3]

Gardez une copie récupérable.

Déterminez ce qu'il faudrait récupérer après une perte, une panne ou une attaque.

01 Choisir les données importantes

Recensez fichiers, photos, documents professionnels et données infonuagiques essentiels. Désignez un responsable et précisez la quantité de travail récent que vous pourriez perdre. Choisissez ensuite la fréquence de sauvegarde. [6, 7]

02 Séparer la sauvegarde

Conservez plusieurs copies, dont une à un autre endroit. Une copie déconnectée peut réduire l'exposition aux rançongiciels. Protégez l'accès aux sauvegardes infonuagiques avec un mot de passe unique et la MFA. [7, 9]

03 Vérifier le résultat

Examinez les échecs et les alertes de stockage. Restaurez un fichier dans un endroit sûr et ouvrez-le. Notez la date, le résultat et la prochaine vérification. Le statut « terminé » ne prouve pas que tous les fichiers sont récupérables. [7]

À RETENIR

La synchronisation ne suffit pas à définir la reprise. Vérifiez l'historique, la conservation, la récupération des fichiers supprimés et le scénario d'un compte compromis. Convenez d'une sauvegarde indépendante pour les données de travail. [7, 8]

VOTRE PROCHAINE VÉRIFICATION

Fichiers ou systèmes importants

Responsable et emplacement de la sauvegarde

Date et résultat du dernier test de restauration

Vous soupçonnez une attaque?

Restez calme. Utilisez un autre appareil fiable pour obtenir de l'aide si votre appareil ou votre courriel peut être compromis.

01

Contenir

En cas de logiciel malveillant ou de rançongiciel présumé, déconnectez l'appareil du Wi-Fi, d'Ethernet et des autres réseaux. Cessez de l'utiliser et joignez les TI. Demandez conseil avant de redémarrer, d'effacer ou de reconnecter l'appareil : la bonne action dépend de l'incident. [9, 11]

02

Protéger les comptes

Depuis un appareil fiable, suivez la procédure officielle de récupération du fournisseur. Réinitialisez le mot de passe et révoquez les sessions. Examinez avec les TI ou le fournisseur la récupération, les méthodes MFA et le transfert des courriels. [10, 11]

03

Documenter et reprendre

Notez de façon sûre l'heure, les systèmes touchés et les messages. Isolez les sauvegardes. Restaurez dans un environnement sain après avoir traité la cause. Si des renseignements financiers sont exposés, joignez l'institution par son canal officiel. [9, 11]

Besoin de préparer votre plan?

Discutez avec DITC des comptes, appareils et sauvegardes. La disponibilité, le périmètre et les frais sont convenus avant le mandat.

ditc.ca | support@ditc.ca | 514 970-5667

SOURCES ET POUR ALLER PLUS LOIN

- | | |
|---|---|
| 1. Mots de passe et phrases de passe | 7. Conseils de sauvegarde et de restauration |
| 2. Authentification multifacteur | 8. Contrôles de sécurité de base |
| 3. Reconnaître l'hameçonnage | 9. Réagir à un rançongiciel |
| 4. Mises à jour logicielles | 10. Récupérer un compte compromis |
| 5. Sécurité des appareils et du Wi-Fi | 11. Contenir un logiciel malveillant |
| 6. Bases pour les petites organisations | 12. Authentification résistante à l'hameçonnage |

Les liens mènent aux conseils officiels canadiens. DITC est indépendant; aucune approbation gouvernementale n'est sous-entendue.

Conseils généraux, sans garantie de sécurité. Suivez vos politiques de travail et obtenez une aide adaptée à votre situation.