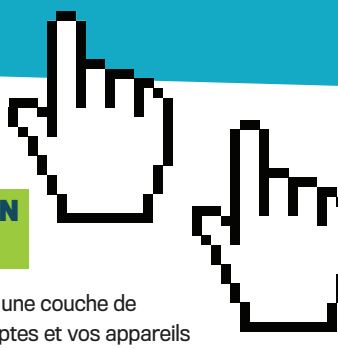
# LE GUIDE DES PME POUR ASSURER LEUR CYBERSÉCURITÉ DURANT LA COVID-19

La pandémie de COVID-19 a complètement bouleversé les activités de nombreuses entreprises. Il est donc plus important que jamais d'assurer la cybersécurité de la vôtre.

La pandémie de COVID-19 nous a montré que le monde peut changer très rapidement, mais la nécessité d'assurer notre cybersécurité, elle, ne change pas. La sensibilisation de vos employés aux pratiques exemplaires en cybersécurité est essentielle pour protéger votre entreprise contre les cyberattaques.



## QUELQUES ÉTAPES SIMPLES POUR PROTÉGER VOTRE MILIEU DE TRAVAIL

### ADOPTEZ UNE POLITIQUE SUR LA CYBERSÉCURITÉ

Il est impossible pour vos employés de connaître toutes les cybermenaces qui les guettent, mais si vous avez établi des règles claires en matière de cybersécurité, ils sauront prendre les bonnes décisions en temps et lieu.

Une politique sur la cybersécurité doit comprendre :

**DES LIGNES DIRECTRICES SUR L'UTILISATION D'INTERNET**

**DES RÈGLES SUR LA SÉCURITÉ DU COURRIEL**

**DES LIGNES DIRECTRICES SUR LES RÉSEAUX SOCIAUX**

### CRÉEZ DES MOTS DE PASSE ROBUSTES

Tous les employés devraient utiliser une **phrase de passe** composée d'au moins 4 mots et 15 caractères.

Ou bien un **mot de passe complexe** :

- Au moins 12 caractères
- Combinaison de majuscules, minuscules, chiffres et symboles
- Aucun renseignement personnel

**UTILISEZ UN MOT DE PASSE UNIQUE POUR CHAQUE COMPTE**

**NE PARTAGEZ JAMAIS VOS MOTS DE PASSE AVEC QUICONQUE**

**CHANGEZ VOS MOTS DE PASSE SI L'UN DE VOS COMPTES A ÉTÉ COMPROMIS**

### ACTIVEZ L'AUTHENTIFICATION MULTIFACTORIELLE

**L'authentification multifactorielle** ajoute une couche de sécurité qui permet de mieux protéger vos comptes et vos appareils en utilisant au moins deux facteurs pour vérifier que vous êtes bien la personne que vous prétendez être. C'est ce qu'on appelle les **facteurs d'authentification**.

Il existe différents types de facteurs d'authentification, dont :

- **Qui vous êtes**, comme vos empreintes digitales ou la reconnaissance faciale
- **Ce que vous connaissez**, comme une question de sécurité ou un mot de passe
- **Ce que vous possédez**, comme une clé USB

Si plusieurs personnes doivent utiliser des appareils et accéder aux comptes de votre entreprise, assurez-vous qu'elles sont en mesure de vérifier leur identité. Vous pouvez contrôler les employés ou les visiteurs qui sont autorisés à accéder à vos comptes.

### NE MORDEZ PAS À L'HAMEÇON

Les entreprises sont une cible de choix pour **les tentatives d'hameçonnage et de harponnage**. Dans le cadre de ces arnaques, les cybercriminels se font souvent passer pour des employés et cherchent à obtenir des renseignements sensibles appartenant à l'entreprise, comme des mots de passe ou de l'information financière.

Si vous recevez un courriel non sollicité, même s'il semble provenir d'un collègue, voici ce que vous devez faire :

**RESPIREZ.** Les messages d'hameçonnage sont conçus pour exercer une pression ou même menacer la victime afin de l'amener à répondre rapidement. Si l'on exige que vous répondiez « immédiatement », il s'agit probablement d'une tentative d'escroquerie.

**NE CLIQUEZ PAS SUR LES LIENS OU LES PIÈCES JOINTES** dont vous n'êtes pas certains. Tentez de joindre l'expéditeur d'une autre manière, par exemple par téléphone, pour confirmer qu'il a bien envoyé le message.

**COMMUNIQUEZ AVEC LES SERVICES TI.** Les messages non sollicités vous demandant de modifier un mot de passe ou de mettre un compte à jour sont fort probablement des tentatives de fraude.

**SUPPRIMEZ TOUT MESSAGE QUI SEMBLE TROP BEAU POUR ÊTRE VRAI,** comme les messages qui vous annoncent que vous avez gagné un concours auquel vous n'avez pas participé.

POUR D'AUTRES CONSEILS SUR LA FAÇON DE VOUS PROTÉGER ET DE PROTÉGER VOTRE ENTREPRISE ET VOS APPAREILS, CONSULTEZ **PENSEZCYBERSECURITE.CA**

SUIVEZ-NOUS SUR LES RÉSEAUX SOCIAUX **@PENSEZCYBERSÉCURITÉ** OU SUR TWITTER **@CYBER_SECURITE**

Centre de la sécurité des télécommunications | Communications Security Establishment | Canada