Guide de réunion

Mot de passe

Présentation de l'activité

cyber eco

Dernière mise à jour : janvier 2026

Objectifs

Animer

une discussion au sein de l'entreprise afin de partager les bases de la sécurité sur le thème abordé.

Encourager

la prise de parole et le partage d'expériences liées à des attaques recourant aux techniques abordées durant l'atelier.

Détails de l'activité

Durée : 20 - 30 minutes

Clientèle visée : l'ensemble des employé(e)s

Objectifs	Responsabilité de la personne qui anime	Responsabilité des employé(e)s	Matériel recommandé
Couvrir les points essentiels du thème abordé	Présenter les questions ou sujets et commenter à l'aide des pistes fournies	Participer activement et répondre aux questions	Projecteur, tableau et marqueurs

Notes à l'intention de la personne animant l'atelier

Nous vous invitons à prendre connaissance des informations ci-dessus et à la page suivante avant d'animer l'atelier, et d'utiliser les notes contenues dans les pages suivantes pour compléter l'information transmises à votre équipe.

Bonne présentation!

Quelles sont les bonnes pratiques à mettre en place dans votre entreprise?

Les entreprises doivent instaurer une politique visant à gérer de façon sécuritaire les mots de passe au sein de l'organisation.

Pour ce faire, il est recommandé de sensibiliser les employé(e)s en continu aux bonnes pratiques ci-dessous :

- Utilisation d'une phrase de passe, à moins que les systèmes ne le permettent pas en raison de restrictions technologiques ou d'anciens systèmes.
- Interdiction d'utiliser des mots de passe peu robustes, contenant moins de 12 caractères ou facile à deviner.
- Partage d'une liste de mots de passe à proscrire (ex. : 12345678, password , P@ssword , soleil123, qwerty123, nom de votre entreprise suivi de 123).
- Rappel aux employés d'évaluer la robustesse des mots de passe qu'ils utilisent au sein de l'entreprise à l'aide des lignes directrices du site Pensez cybersécurité (gouvernement du Canada).

Vous trouverez ci-dessus des pratiques de sécurité à mettre en place au sein de votre entreprise. Nous vous conseillons d'en prendre connaissance avant la tenue de l'atelier avec les employé(e)s.

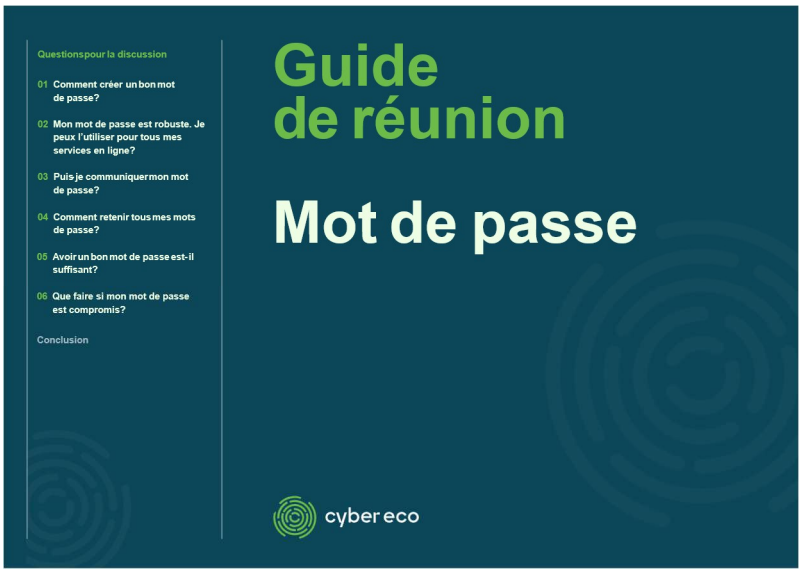
Pour toute information additionnelle ou tout conseil spécifique, nous vous recommandons de consulter l'expert en informatique de votre organisation ou une firme de consultation en informatique.

Que vous soyez gestionnaire, propriétaire ou responsable des TI, voici des références qui pourront vous aider dans la bonne gestion des mots de passe au sein de votre organisation.

1- Gérer ses mots de passe | Gouvernement du Québec

2- Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032) - Centre canadien pour la cybersécurité

3- Votre mot de passe est-il suffisamment robuste? Voici cinq façons de l'évaluer - Pensez cybersécurité



Bonjour et bienvenue à cet atelier!

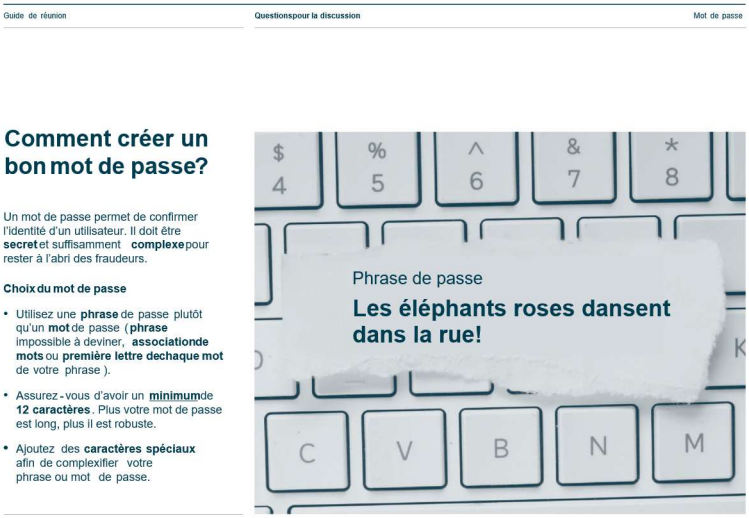
Aujourd'hui, nous allons parler de **mots de passe**.

L'atelier devrait durer 20 à 30 minutes. Votre participation et vos questions sont essentielles!

Les mots de passe sont **essentiels**. C'est important d'en parler pour assurer la **protection** et la **confidentialité** des **informations personnelles** et **professionnelles** que nous détenons. Tant pour **notre clientèle** que pour **notre entreprise**.

Les mots de passe sont aussi essentiels pour avoir une **barrière efficace contre les cyberattaques** et donc pour **prévenir la fraude**.

Aujourd'hui, nous allons aborder les six questions qui s'affichent à gauche de l'écran.



Page 2 [Lire le contenu de la diapo]

Première question : Comment créer un bon mot de passe?

Notes additionnelles

Un mot de passe robuste est la **première ligne de défense** pour protéger des informations personnelles et professionnelles.

Quelques conseils

- Si le système n'impose pas un maximum de caractères, utilisez une **phrase de passe**. Elle peut être sérieuse, ludique ou liée à quelque chose que vous aimez. Par exemple :
  - Les éléphants roses dansent dans la rue! / Le Bonhomme carnaval aime les chips au BBQ!
- Utilisez une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux. Même si le système n'exige pas de caractères spéciaux, on vous encourage à en mettre.
- Évitez les mots courants comme le nom de notre entreprise, les informations personnelles (nom, date de naissance) ou les séquences faciles à deviner (12345678, motdepasse).
- Ne partagez **jamais** votre mot de passe et ne le rendez **pas** accessible en le notant sur un bout de papier.

Bon à savoir : il n'est **PAS** recommandé de modifier régulièrement un mot de passe, surtout s'il est robuste.

En conclusion : Plus votre mot de passe est robuste, plus les fraudeurs auront de la difficulté à le pirater!

Page 3 [Lire le contenu de la diapo]

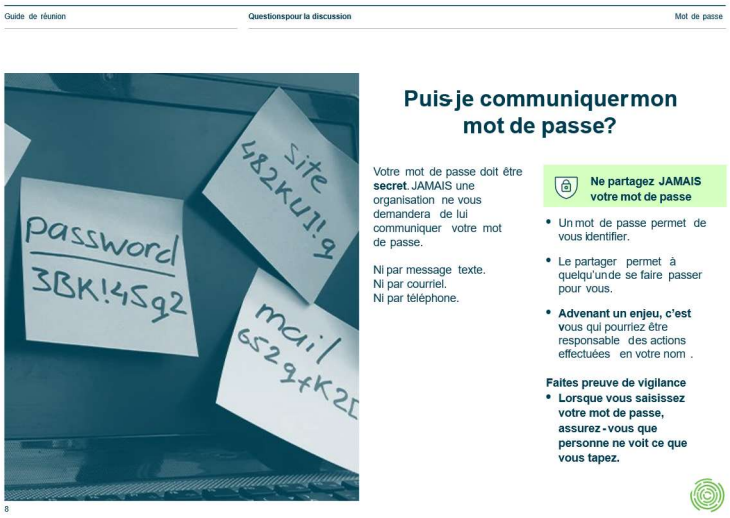
Deuxième question : Mon mot de passe est robuste. Je peux l'utiliser pour tous mes services en ligne?

Notes additionnelles

Si un fraudeur met la main sur votre mot de passe, et que vous utilisez ce **même** mot de passe pour **plusieurs** services, **tous** ces services sont à risque.

Une fois le mot de passe connu, les fraudeurs l'utilisent pour tenter de se connecter à la multitude de services que vous utilisez.

LA chose à retenir : il faut avoir autant **UN** mot de passe pour **CHAQUE** service en ligne.



Page 4 [Lire le contenu de la diapo]

Troisième question : Puis-je communiquer mon mot de passe?

Notes additionnelles

Votre mot de passe doit être **secret**.

S'il est partagé, vous perdez le contrôle sur son utilisation. Advenant qu'il soit utilisé de façon malveillante, vous pourriez être tenu(e) responsable des conséquences.

Dites-vous aussi que même une personne de confiance peut, par inadvertance, compromettre votre mot de passe.

La même consigne s'applique aussi pour le partage des mots de passe **entre collègues**. Cette pratique n'est **PAS** recommandée.

Page 5 [Lire la mise en situation de la diapo]

Quatrième question : Comment retenir tous mes mots de passe?

Notes additionnelles

Il est impossible de retenir tous nos mots de passe.

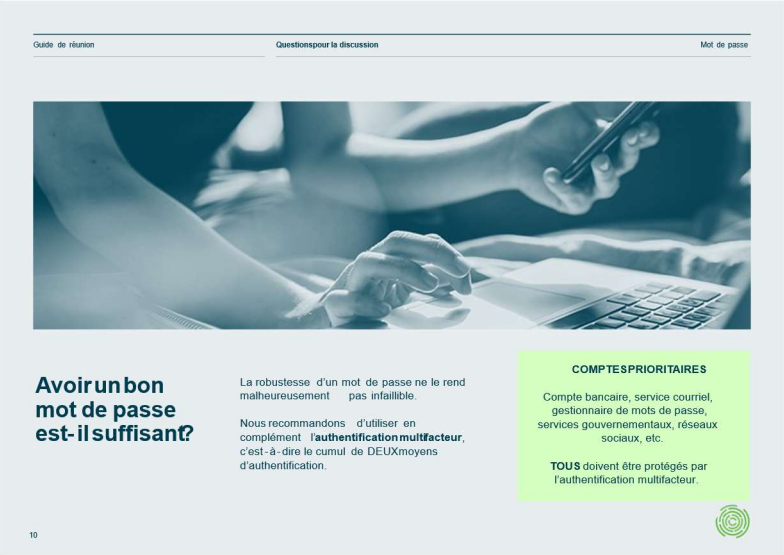
Ne commettez surtout pas l'erreur :

- de les noter sur un bout de papier
- de les inscrire dans votre messagerie ou dans un fichier non protégé de votre ordinateur
- ou de les garder dans votre téléphone mobile, advenant qu'un fraudeur y ait éventuellement accès

Apprenez à utiliser un gestionnaire de mot de passe sécurisé pour qu'il s'en charge à votre place. Vous n'aurez plus qu'à retenir le mot de passe maître de votre gestionnaire.

Bon à savoir : Pour choisir un bon gestionnaire de mots de passe, référez-vous aux conseils du Gouvernement du Québec

- **Critères pour choisir une gestionnaire de mots de passe sécuritaire et efficace :** Comment sécuriser ses mots de passe? | Gouvernement du Québec



Page 6 [Lire le contenu de la diapo]

Cinquième question : Avoir un bon mot de passe est-il suffisant?

Notes additionnelles

L'authentification multifacteur, ou authentification double facteurs (2FA), **ajoute** une **couche de protection** à votre compte. Elle exige **deux éléments distincts** pour confirmer votre identité :

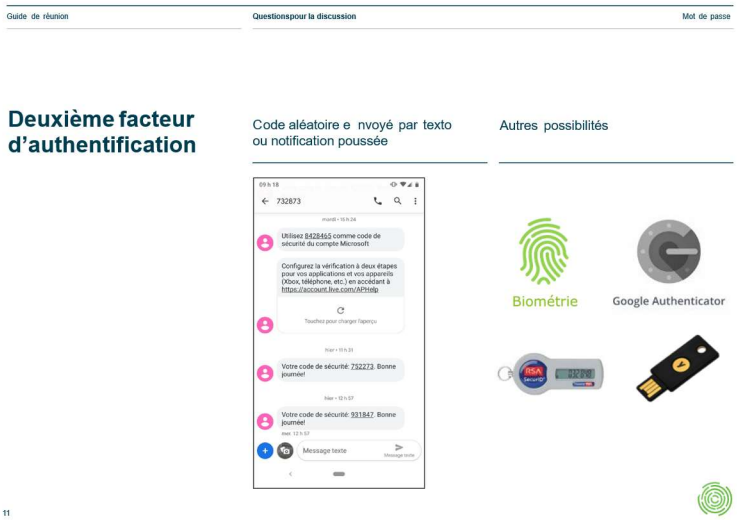
1. **Quelque chose que vous connaissez** : votre mot de passe.
2. **Quelque chose que vous possédez** : un code temporaire envoyé par SMS, une application d'authentification (comme Microsoft Authenticator ou Google Authenticator) ou une clé physique.

Les avantages

- **Renforce la sécurité** : même si votre mot de passe est compromis, un fraudeur ne pourra pas accéder à votre compte sans le second facteur.

- **Protège vos données sensibles** : particulièrement utile pour les comptes professionnels, bancaires ou contenant des informations personnelles.

- **Réduit les risques de piratage** : les attaques par hameçonnage ou les fuites de mots de passe deviennent moins efficaces.



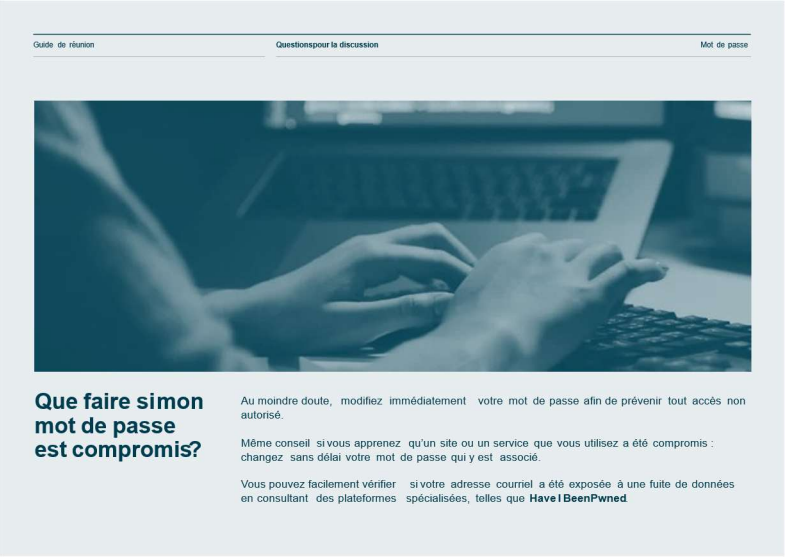
Page 7 [Lire le contenu de la diapo]

Notes additionnelles : authentification multifacteur

En plus de notre mot de passe, un code aléatoire - ou code à usage unique - peut être envoyé par texto ou par notification poussée sur un appareil. Il faut alors saisir ce code dans l'application à laquelle on souhaite se connecter.

Il existe d'autres types de 2e facteur d'authentification, principalement la biométrie, google authentificator ou une clé de sécurité.

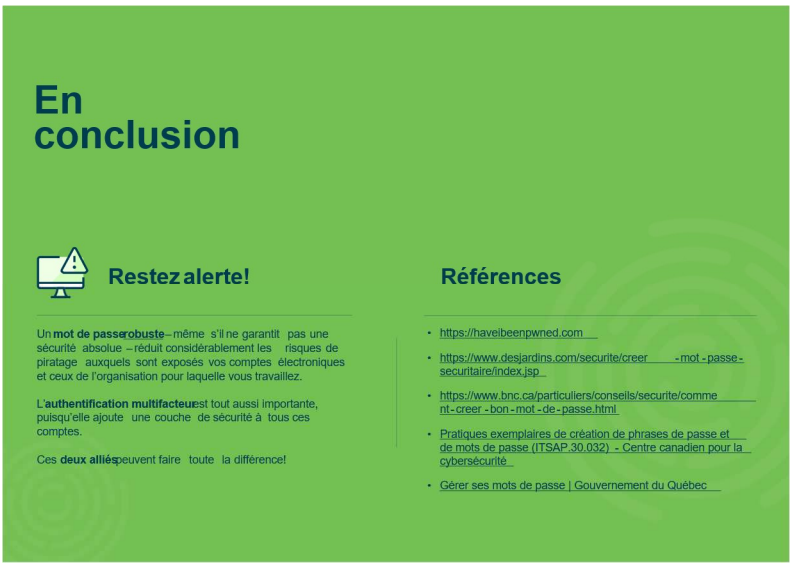
Bon à savoir : Une clé de sécurité est un périphérique physique (souvent ressemblant à une clé USB) qui sert de facteur d'authentification supplémentaire pour protéger vos comptes en ligne, ou un mot de passe réseau (parfois appelé clé Wi-Fi) pour vous connecter à un réseau sans fil.



Page 8 [Lire le contenu de la diapo]

Sixième question : Que faire si mon mot de passe est compromis? [Lire le contenu de la diapo]

Bon à savoir : le site “**Have I Been Pwned**” est facile à utiliser. Il suffit d’y entrer une adresse courriel et le diagnostique est quasi instantané. Une référence à partager avec les collègues et nos proches!



Page 12 [Lire le contenu de la diapo]

En conclusion

Pour en apprendre davantage, les références ci-dessus vous seront très utiles.

J'espère que l'atelier vous en a appris davantage sur les mots de passe et l'importance de bien se protéger, autant dans notre entreprise que dans notre vie privée.

Merci d'avoir participé à l'atelier!

Annexe

Temps nécessaire à un pirate pour forcer votre mot de passe en 2025

Matériel : 12 x RTX 5090 \ Hachage de mot de passe : bcrypt (10)

Nombre de caractères	Nombre seulement	Lettres minuscules	Lettres majuscules et minuscules	Chiffres, lettres majusculeset minuscules	Chiffres, lettres majusculeset minuscules, symboles
4	Immédiatement	Immédiatement	Immédiatement	Immédiatement	Immédiatement
5	Immédiatement	Immédiatement	57 minutes	2 heures	4 heures
6	Immédiatement	46 minutes	2 jours	6 jours	2 semaines
7	Immédiatement	20 heures	4 mois	1 an	2 ans
8	Immédiatement	3 semaines	15 ans	62 ans	164 ans
9	2 heures	2 ans	791 ans	3K ans	11k ans
10	1 jour	40 ans	41k ans	238 ans	803 ans
11	1 semaine	1k d'années	2 millions d'années	14 millions d'années	56 millions d'années
12	3 mois	27k années	111 millions d'années	917 millions d'années	3 milliards d'années
13	3 ans	705k années	5 milliards d'années	56 milliards d'années	275 milliards d'années
14	28 ans	18 millions d'années	300 milliards d'années	3 billions d'années	19 billions d'années
15	284 ans	477 millions d'années	15 billions d'années	218 billions d'années	1 quintillions d'années
16	2 000 ans	12 milliards d'années	812 quintillions d'années	13 quadrillions d'années	94 quadrillions d'années
17	28 000 ans	322 milliards d'années	42 quadrillions d'années	840 quadrillions d'années	6 quintillions d'années
18	284 000 ans	8 quintillions d'années	2 quintillions d'années	52 quintillions d'années	463 quintillions d'années

Référence: https://www.hivesystems.com/blog/are-your-passwords-in-the-green

Ce tableau démontre la facilité avec laquelle les fraudeurs réussissent à découvrir un mot de passe lorsque celui-ci n'est pas robuste.