

Guide de réunion

Mot de passe

Présentation de l'activité

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

Cible 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



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).



Questions pour la discussion

- 01 Comment créer un bon mot de passe?
- 02 Mon mot de passe est robuste. Je peux l'utiliser pour tous mes services en ligne?
- 03 Puis-je communiquer mon mot de passe?
- 04 Comment retenir tous mes mots de passe?
- 05 Avoir un bon mot de passe est-il suffisant?
- 06 Que faire si mon mot de passe est compromis?

Conclusion

Guide de réunion

Mot de passe

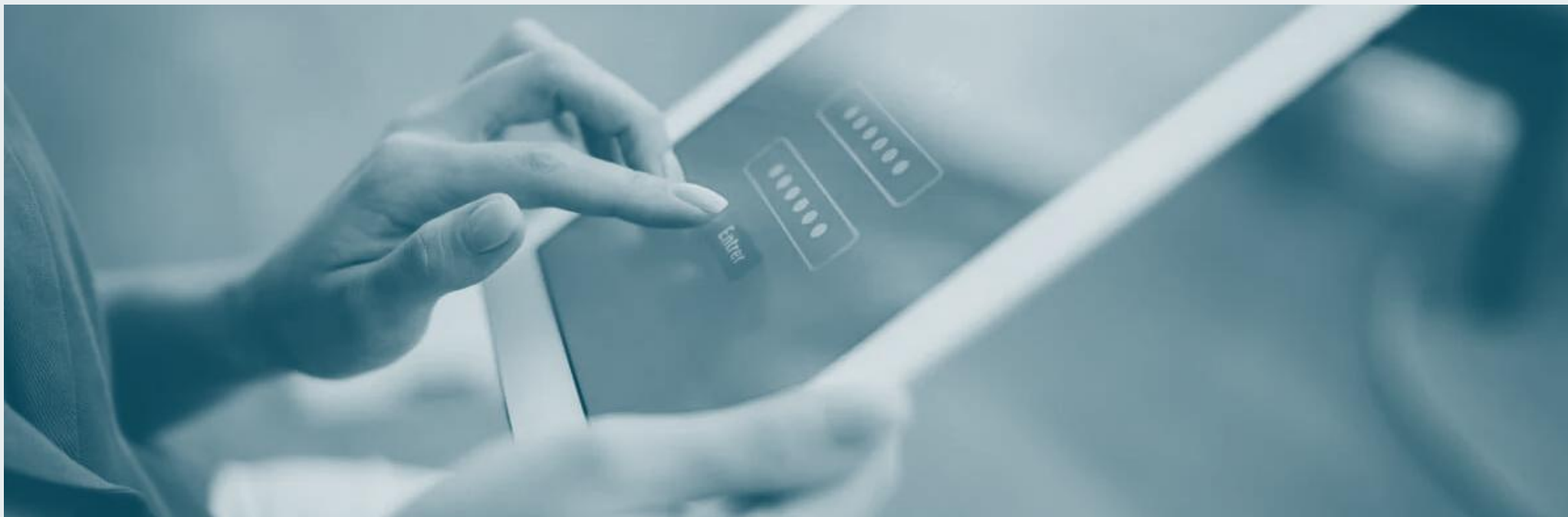
Comment créer un bon mot de passe?

Un mot de passe permet de confirmer l'identité d'un utilisateur. Il doit être **secret** et suffisamment **complexe** pour rester à l'abri des fraudeurs.

Choix du mot de passe

- Utilisez une **phrase** de passe plutôt qu'un **mot** de passe (**phrase impossible à deviner, association de mots** ou **première lettre de chaque mot** de votre phrase).
- Assurez-vous d'avoir un **minimum** de **12 caractères**. Plus votre mot de passe est long, plus il est robuste.
- Ajoutez des **caractères spéciaux** afin de complexifier votre phrase ou mot de passe.





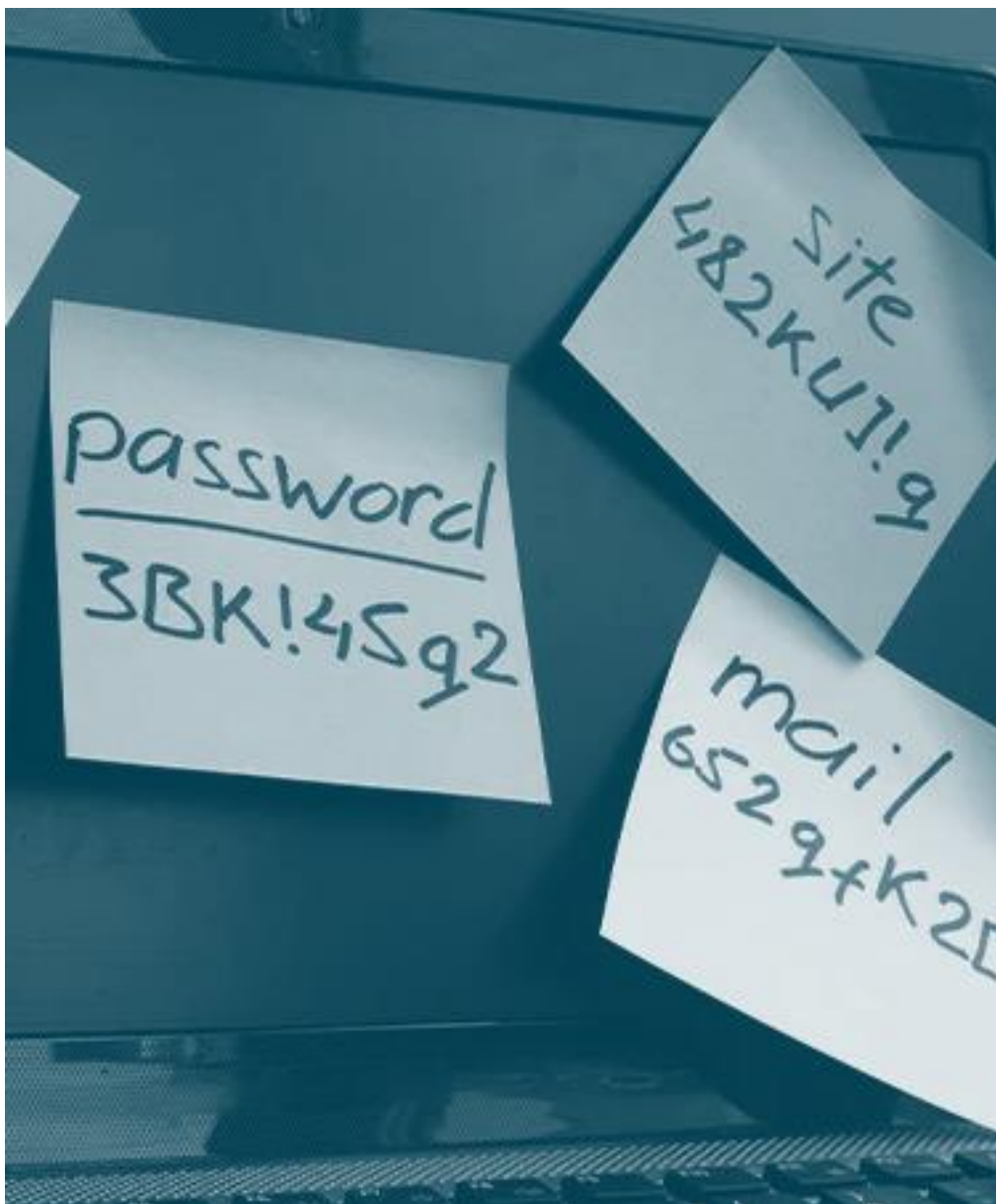
Mon mot de passe est robuste. Je peux l'utiliser pour tous mes services en ligne?

Non! On doit utiliser un mot de passe différent pour chaque service en ligne (comptes bancaires, LinkedIn, Gmail, Facebook, X, Netflix, etc.).

Pourquoi? Parce qu'en cas de piratage, seul le service associé au mot de passe compromis sera vulnérable.

1 MOT DE PASSE : 1 SERVICE EN LIGNE





Puis-je communiquer mon mot de passe?

Votre mot de passe doit être **secret**. JAMAIS une organisation ne vous demandera de lui communiquer votre mot de passe.

Ni par message texte.
Ni par courriel.
Ni par téléphone.



Ne partagez JAMAIS votre mot de passe

- Un mot de passe permet de vous identifier.
- Le partager permet à quelqu'un de se faire passer pour vous.
- Advenant un enjeu, c'est vous qui pourriez être responsable des actions effectuées en votre nom.

Faites preuve de vigilance

- Lorsque vous saisissez votre mot de passe, assurez-vous que personne ne voit ce que vous tapez.



Comment retenir tous mes mots de passe?

Une façon sécuritaire et efficace de *gérer* – et non *retenir* – vos mots de passe consiste à utiliser un **gestionnaire de mots de passe**, qui se chargera de :

- Stocker, de façon sécuritaire et centralisée, tous vos mots de passe.
- Générer automatiquement des mots de passe robustes.
- Protéger, par un mot de passe maître, l'ensemble de vos mots de passe.

Vous n'avez ainsi qu'un seul mot de passe à retenir. Il doit toutefois respecter les meilleures pratiques, car il donne accès à l'ensemble de vos mots de passe. Un bon mot de passe maître vous garantira une utilisation optimale de ce type d'outil.





Avoir un bon mot de passe est-il suffisant?

La robustesse d'un mot de passe ne le rend malheureusement pas infaillible.

Nous recommandons d'utiliser en complément l'**authentification multifacteur**, c'est-à-dire le cumul de DEUX moyens d'authentification.

COMPTES PRIORITAIRES

Compte bancaire, service courriel, gestionnaire de mots de passe, services gouvernementaux, réseaux sociaux, etc.

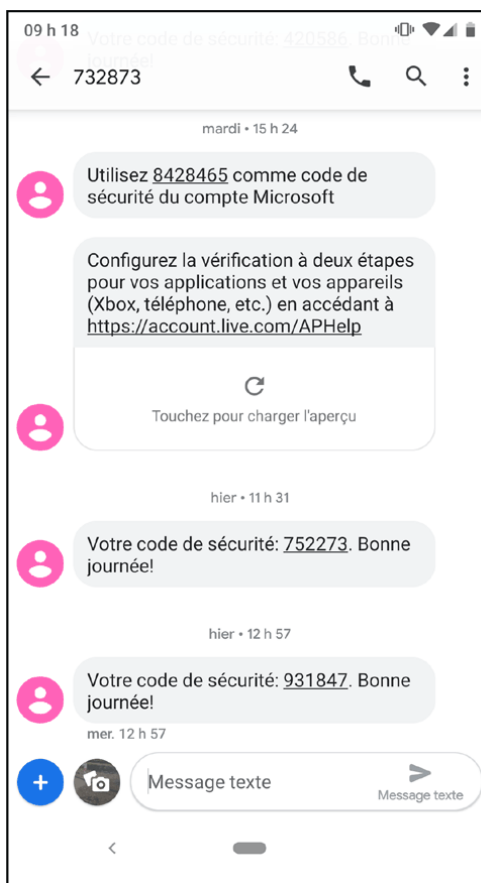
TOUS doivent être protégés par l'authentification multifacteur.



Deuxième facteur d'authentification

Code aléatoire envoyé par texto ou notification poussée

Autres possibilités



Biométrie



Google Authenticator





Que faire si mon mot de passe est compromis?

Au moindre doute, modifiez immédiatement votre mot de passe afin de prévenir tout accès non autorisé.

Même conseil si vous apprenez qu'un site ou un service que vous utilisez a été compromis : changez sans délai votre mot de passe qui y est associé.

Vous pouvez facilement vérifier si votre adresse courriel a été exposée à une fuite de données en consultant des plateformes spécialisées, telles que **Have I Been Pwned**.

En conclusion



Restez alerte!

Un **mot de passe robuste** – même s’il ne garantit pas une sécurité absolue – réduit considérablement les risques de piratage auxquels sont exposés vos comptes électroniques et ceux de l’organisation pour laquelle vous travaillez.

L’**authentification multifacteur** est tout aussi importante, puisqu’elle ajoute une couche de sécurité à tous ces comptes.

Ces **deux alliés** peuvent faire toute la différence!

Références

- <https://haveibeenpwned.com>
- <https://www.desjardins.com/securite/creer-mot-passe-securitaire/index.jsp>
- <https://www.bnc.ca/particuliers/conseils/securite/comment-creer-bon-mot-de-passe.html>
- [Pratiques exemplaires de création de phrases de passe et de mots de passe \(ITSAP.30.032\) - Centre canadien pour la cybersécurité](#)
- [Gérer ses mots de passe | Gouvernement du Québec](#)

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 majuscules et minuscules	Chiffres, lettres majuscules et 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



Licence et Avertissement

Sujet au respect des termes et conditions de cette licence, Cybereco vous octroie le droit gratuit et non-exclusif d'utiliser et de reproduire ce matériel à des fins internes ainsi que de le partager selon les mêmes termes et conditions. Le matériel ne peut être modifié et la marque de Cybereco et les termes et conditions de cette licence doivent y demeurer apposés tels quels.

Cette licence ne vous permet pas de revendiquer quelque droit de propriété intellectuelle dans le matériel, de le vendre ou d'utiliser toute marque de commerce qui y est contenue séparément sans l'autorisation de son propriétaire.

Les renseignements contenus dans ce matériel sont d'ordre général seulement et ne constituent pas des conseils ou de services professionnels. Avant de prendre une décision ou de prendre des mesures qui pourraient avoir une incidence sur vos finances ou vos activités, vous devriez consulter un conseiller professionnel qualifié.

Ce matériel est mis à votre disposition « tel quel » et sans aucune garantie. Sans limiter la portée de ce qui précède, Cybereco ne garantit pas que le matériel puisse être utilisé conformément à l'usage auquel il est destiné, qu'il ne contient aucune erreur, ni aucun virus ou programme malveillant, ni qu'il répond à des critères précis en matière de sécurité, de rendement ou de qualité.

Toute garantie implicite de qualité marchande, de caractère approprié à une fin donnée, de titre

et à l'absence de violation de droits de propriété intellectuelle, à la compatibilité, à la sécurité et à l'exactitude est expressément rejetée.

L'utilisation de ce matériel est à vos propres risques, et c'est à vous d'assumer la pleine responsabilité et de toute perte résultant de cette utilisation, y compris, sans s'y restreindre, toute interruption de services ou perte de données. Nous n'assumerons aucune responsabilité à l'égard de dommages-intérêts directs, indirects, spéciaux, accessoires, consécutifs ou punitifs, ni d'aucun autre dommage quel qu'il soit, que ce soit dans une action en justice recherchant une responsabilité contractuelle, juridique ou délictuelle (y compris, sans s'y restreindre, la négligence) ou autrement, relativement à l'utilisation de ce matériel même si nous étions, ou aurions dû être, au courant de la possibilité des dommages.

Certains liens de cette trousse font référence à des sites web ou articles qui ne sont pas sous le contrôle de Cybereco. Cybereco n'est pas responsable du contenu de ces sites web, ni des informations, logiciels, produits et services disponibles sur ou par l'intermédiaire de ces sites. Les liens sélectionnés sont uniquement destinés à fournir un complément d'information. Cybereco n'assume aucune obligation ou responsabilité de quelque nature que ce soit à cet égard.

Cette exonération de responsabilité vaut pour Cybereco et chacun des membres Cybereco ainsi qu'à notre personnel, nos consultants et à leur personnel et leurs consultants respectifs.