Guide de réunion

Mot de passe

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 MATERIEL 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 MATERIEL EST MIS A VOTRE DISPOSITION « TEL QUEL » ET SANS AUCUNE GARANTIE. SANS LIMITER LA PORTÉE DE CE QUI PRÉCÈDE, CYBERECO NE GARANTIT PAS QUE LE MATERIEL PUISSE ÊTRE UTILISÉ CONFORMÉMENT À L'USAGE AUQUEL IL EST DESTINE, QU'IL NE CONTIENT AUCUNE ERREUR, NI AUCUN VIRUS OU PROGRAMME MALVEILLANT, NI QU'IL RÉPOND À DES CRITÈRES PRÉCIS EN MATIÈRE DE SECURITÉ, 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 REJETTÉE.

Licence et Avertissement

L'UTILISATION DE CE MATERIEL 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 MATERIEL 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. »

Présentation de l'activité

cyber eco

OBJECTIFS

ANIMER

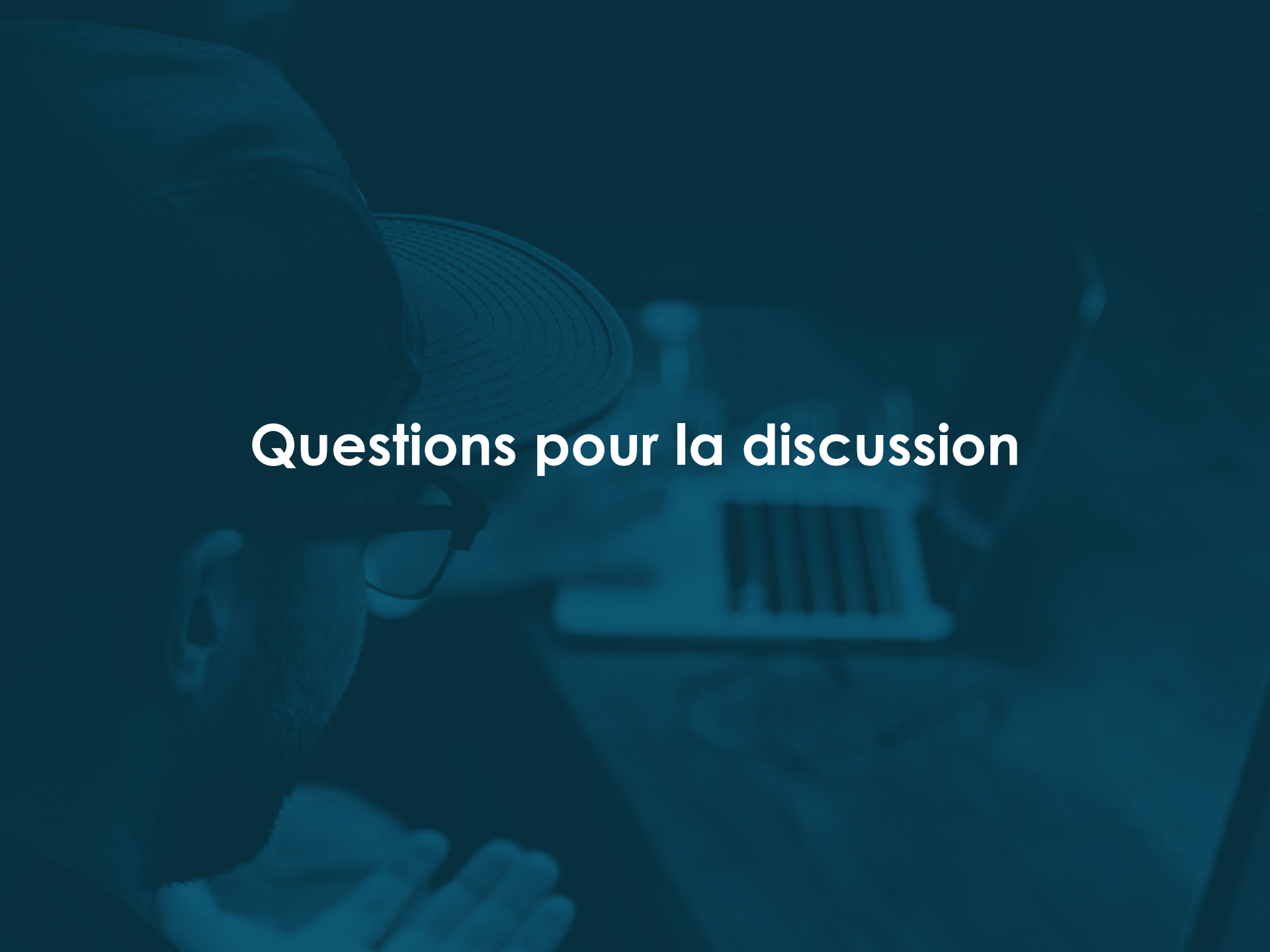
une discussion au sein de l'entreprise afin de partager les connaissances relatives au thème abordé.

ENCOURAGER

la prise de parole et le partage d'expériences relatifs à des attaques utilisant les techniques abordées par le thème de la discussion.

DÉTAILS DE L'ACTIVITÉ

Durée	Objectifs	Responsabilités de l'animateur	Responsabilités des employés	Matériels
10 - 20 minutes	Couvrir brièvement les points essentiels du thème abordé dans le guide	Présenter et commenter les réponses aux questions	Répondre aux questions	Projecteur tableau interactif et marqueurs



Questions pour la discussion

Questions pour la discussion

01	Comment créer un bon mot de passe?
02	Un bon mot de passe peut-il être utilisé pour tous mes services en ligne?
03	Puis-je communiquer mon mot de passe?
04	Comment retenir tous mes mots de passe?
05	Au sein des entreprises, quelles sont les bonnes pratiques à mettre en place?
06	Avoir un bon mot de passe est-il suffisant?

Comment créer un bon mot de passe?

Un mot de passe permet de confirmer l'identité d'un utilisateur. Le mot de passe doit être suffisamment **complexe et secret** pour qu'il soit difficile à un fraudeur de le deviner ou le découvrir.

CHOIX DU MOT DE PASSE

Utiliser des PHRASES DE PASSE au lieu des MOTS de passe

- Une phrase de passe est une **association de mots ou une phrase** ayant du sens juste pour vous et que personne d'autre ne saurait deviner.

- Plus c'est long, mieux c'est. Privilégiez les phrases de passe qui atteignent **21 caractères**. Ce nombre peut-être facilement atteint en associant 4 mots ou en créant une phrase illogique.

- Exemple : Créez une PHRASE de passe en associant des éléments de votre quotidien n'ayant pas de liens évidents **« ChatMarcherCuillereOrange ».**

NB : si le système l'oblige, vous devez ajouter un caractère spécial, un chiffre ou une majuscule.

Un seul mot de passe peut-il être utilisé pour tous mes services en ligne?

Non! Utilisez un mot de passe différent pour chaque service en ligne (ex. : LinkedIn, Facebook, Google, Twitter, comptes bancaires, Netflix, Amazon, Yahoo, etc.). Ainsi, en cas de vol, seul le service associé au mot de passe compromis sera vulnérable.

Alors que si vous utilisez le même mot de passe pour tous vos services en ligne, le vol de celui-ci pourrait compromettre l'ensemble de vos services en ligne. Sachez que les fraudeurs utilisent des mots de passe volés pour effectuer des tentatives de connexions sur une multitude de services en ligne.

Ne mettez donc pas tous vos œufs dans le même panier et ayez autant de mots de passe que vous avez de services en ligne.

1 MOT DE PASSE : 1 SERVICE EN LIGNE

Puis-je communiquer mon mot de passe?

Votre mot de passe doit être secret. Aucune organisation ne vous demandera de lui communiquer votre mot de passe que ce soit par messagerie texte, courriel ou téléphone.

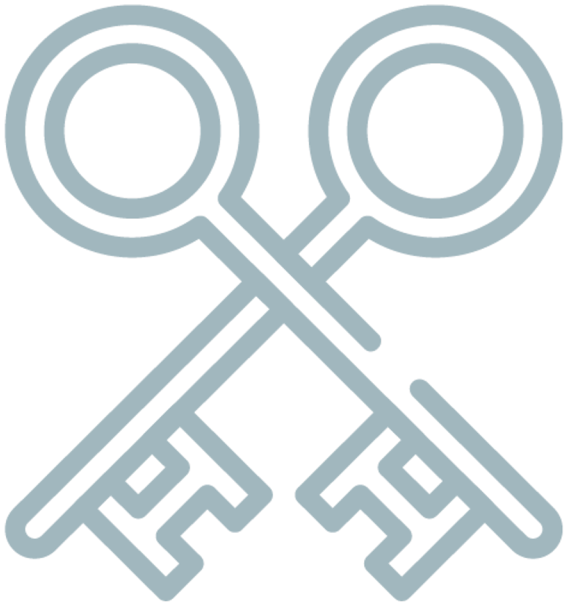
Ne partagez JAMAIS votre mot de passe

- Vos mots de passe permettent de vous identifier, les partager permettrait à d'autres personnes de se faire passer pour vous.

- Vous serez tenus responsable pour les actions effectuées avec votre compte.

Protégez-vous lorsque vous saisissez votre mot de passe

- Soyez vigilant lorsque vous saisissez vos mots de passe et assurez-vous que personne ne peut voir ce que vous tapez.



Comment retenir tous mes mots de passe?

Il est impossible de retenir les dizaines de mots de passe longs et complexes que vous êtes amenés à utiliser quotidiennement. Ne commettez pas pour autant l'erreur de les noter sur un pense-bête, ni de les inscrire dans votre messagerie ou dans un fichier non protégé de votre ordinateur, ou encore dans votre téléphone mobile auquel un cybercriminel pourrait avoir accès.

Apprenez à utiliser un gestionnaire de mot de passe sécurisé qui s'en chargera à votre place, pour ne plus avoir à retenir que le seul mot de passe qui permet d'en ouvrir l'accès.

En résumé, un gestionnaire de mot de passe c'est :

- Un stockage de façon sécuritaire et centralisé de tous vos mots de passe.
- Un outil qui génère des mots de passe forts automatiquement.
- Un outil protégé par un mot de passe maître. Le seul que vous avez à mémoriser. Il doit néanmoins respecter les meilleures pratiques, car il donne l'accès à tous vos autres mots de passe. Un bon mot de passe maître vous garantira une utilisation optimale de ce type d'outil.

Quelques exemples de **gestionnaires de mot de passe** : LastPass, 1password, etc. Ces solutions sont citées seulement à titre d'exemple, et non pas à titre de recommandation.

En entreprise, quelles sont les bonnes pratiques à mettre en place?

Les entreprises doivent instaurer une politique en vue de gérer de façon sécuritaire les mots de passe au sein de leur organisation. Il est recommandé d'implanter une **politique de mots de passe** claire qui respecte au mieux les caractéristiques suivantes :

- Sensibilisez vos employés aux bonnes pratiques (ex. : affiche, aide-mémoire, vidéo, Quiz fournis dans cette Trousse).
- Utilisez la **phrase de passe** lorsque les systèmes le permettent. (restrictions technologiques, anciens systèmes).
- Interdire l'utilisation des mots de passe les plus utilisés (mise en place d'une liste de mots de passe à proscrire. Ex. : password, soleil123, etc.).
- Ne demandez plus le renouvellement de mots de passe à vos employés sauf s'ils ont été découverts par les tests ou s'il y a un risque de compromission. Ceci afin de favoriser la création d'un mot de passe fort dès le départ.
- Testez régulièrement la **robustesse des mots de passe** utilisés dans l'entreprise.
- Mettez en place l'authentification double facteur pour les applications les plus sensibles.

Avoir un bon mot de passe est-il suffisant?

La robustesse des mots de passe ne les rend pas infaillibles pour autant (ex. : en cas de vol de mot de passe). Nous préconisons d'utiliser, en complément, une **authentification double facteur**, c'est-à-dire le cumul de 2 moyens d'authentifications.

PAR EXEMPLE

- **Un mot de passe + un code aléatoire** généré par une application ou envoyé par texto sur votre téléphone intelligent.

- **Un mot de passe + des données biométriques** comme des empreintes pour pouvoir accéder par exemple à un lieu sensible.

COMPTES PRIORITAIRES
Les comptes tels que les comptes bancaires, courriels, les gestionnaires de mots de passe, les réseaux sociaux, doivent prioritairement être protégés par l'authentification double facteur.

Illustrations de deuxième facteur d'authentification

Exemple de code aléatoire envoyé par texto sur votre téléphone intelligent

Autres exemples de deuxième facteur

Biométrie

Google Authenticator

Conclusion

Le choix d'un bon mot de passe, même s'il ne vous garantit pas une sécurité absolue, vous permettra de **réduire les risques de piratage** auxquels sont exposés vos comptes électroniques et cela peut faire la différence.

Vous êtes maintenant outillé, à l'aide de méthodes simples, pour choisir un bon mot de passe, le stocker en toute sécurité et le gérer.

Enfin, l'**authentification à double facteur** vous permettra d'ajouter une couche de sécurité supplémentaire pour la protection de vos comptes.

N'OUBLIEZ PAS!

Vous êtes une **ligne de défense importante** pour protéger notre entreprise!