Atelier – Créer et stocker des mots de passe fiables (Version du formateur)

**Remarque à l’intention du formateur :** le texte en rouge ou surligné en gris apparaît uniquement dans la version du formateur.

1. Objectifs

Comprendre les concepts d’un mot de passe fiable.

Partie 1 : Découvrir les concepts de la création d’un mot de passe fiable.

Partie 2 : Découvrir les concepts du stockage sécurisé de votre mot de passe ?

1. Contexte/scénario

Les mots de passe sont très usités dans la sécurisation de l’accès aux ressources. Les pirates utiliseront de nombreuses techniques pour déchiffrer les mots de passe des utilisateurs et pour obtenir un accès non autorisé aux ressources et données.

Pour mieux vous protéger, il est important de comprendre ce qu’est un mot de passe fiable et comment le stocker en toute sécurité.

1. Ressources requises

* Ordinateur personnel ou terminal mobile avec accès Internet

1. Créer un mot de passe fiable

Les mots de passe fiables se caractérisent par quatre critères principaux énumérés par ordre d’importance :

* + - 1. L’utilisateur peut facilement se rappeler son mot de passe.
      2. Une tierce partie ne doit pas aisément déchiffrer le mot de passe.
      3. Un programme ne doit pas aisément déchiffrer ou identifier le mot de passe.
      4. Il doit être complexe, contenir des chiffres, des symboles et une combinaison de majuscules et de minuscules.

Selon la liste ci-dessus, le premier critère est probablement le plus important, puisque vous devez vous rappeler de votre mot de passe. Par exemple, le mot de passe **#4ssFrX^-aartPOknx25\_70!xAdk<d!** est jugé fiable, puisqu’il répond aux trois derniers critères, mais est très difficile à se rappeler.

De nombreuses entreprises exigent que les mots de passe contiennent une combinaison de nombres, de symboles et de majuscules et de minuscules. Les mots de passe qui sont conformes à cette politique sont adaptés, tant que les utilisateurs peuvent facilement se le rappeler. Voici un exemple de politique relative au mot de passe défini pour une entreprise typique :

* Le mot de passe doit contenir au moins 8 caractères
* Le mot de passe doit contenir des majuscules et des minuscules
* Le mot de passe doit contenir un chiffre
* Le mot de passe doit contenir un caractère non alphanumérique

Prenez un moment pour analyser les caractéristiques d’un mot de passe fiable et la politique courante relative au mot de passe indiqués ci-dessus. Pourquoi l’ensemble de politiques néglige-t-il les deux premiers critères ? Expliquez votre réponse.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

L’utilisateur a plus de difficultés à retenir un mot de passe lorsqu’on y ajoute des symboles, des chiffres et que l’on combine majuscules et minuscules. D’habitude, lorsqu’un utilisateur considère qu’un mot de passe est conforme à un ensemble spécifique de politiques relatives au mot de passe, il réutilisera la même structure, ou même ledit mot de passe dans d’autres services. Certains systèmes exigeront également que l’utilisateur modifie le mot de passe fréquemment, pour éviter que les anciens mots de passe ne soient réutilisés. Ces utilisateurs ne feront certainement que des modifications mineures au mot de passe, au lieu d’en créer un nouveau qui soit toujours conforme aux politiques définies relatives au mot de passe.

La meilleure méthode pour créer des mots de passe fiables consiste à choisir quatre mots aléatoires, ou plus, et de les regrouper. Le mot de passe **televisionfrogbootschurch** est plus fiable que **J0n@than#81**. Remarquez que si le second mot de passe est conforme aux politiques indiquées ci-dessus, les programmes de cryptage de mots de passe arrivent facilement à déchiffrer ce type de mot de passe. Quoique de nombreux ensembles de politiques relatives au mot de passe ne valident pas le premier mot de passe, **televisionfrogbootschurch**, il est plus fiable que le second. Il est plus facile à se rappeler pour l’utilisateur (surtout en étant associé à une image), il est plus long et son facteur aléatoire le rend plus difficile à déchiffrer par les perceurs de mots de passe.

Créez des mots de passe grâce à un outil de création de mot de passe en ligne, selon l’ensemble de politiques courantes en entreprise relatives au mot de passe indiqué ci-dessus.

* + 1. Ouvrez un navigateur Web et accédez à l’adresse [http://passwordsgenerator.net](http://passwordsgenerator.net/).
    2. Sélectionnez les options conformes à l’ensemble de politiques relatives au mot de passe.
    3. Générez le mot de passe.

Le mot de passe généré est-il facile à se rappeler ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Plusieurs réponses sont possibles. Il est certain que le mot de passe n’est pas facile à se rappeler.

Créez des mots de passe grâce à un outil de création de mot de passe en ligne, selon des mots aléatoires. Remarquez que les mots étant liés, ils ne sont pas dans le dictionnaire.

* + 1. Ouvrez un navigateur Web et accédez à l’adresse   
       <http://preshing.com/20110811/xkcd-password-generator/>.
    2. Générez un mot de passe comprenant des mots aléatoires en cliquant sur **Generate Another!** (Générer un nouveau !) dans la partie supérieure de la page Web.
    3. Le mot de passe généré est-il facile à se rappeler ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Plusieurs réponses sont possibles. Il est certain que le mot de passe est facile à se rappeler.

1. Stocker les mots de passe en toute sécurité

Si l’utilisateur choisit d’utiliser un administrateur de mots de passe, la première caractéristique d’un mot de passe fiable peut être ignorée, puisque l’utilisateur peut accéder à l’administrateur de mots de passe à tout moment. Remarquez que certains utilisateurs gardent leur mot de passe uniquement dans leur mémoire. Les administrateurs de mots de passe, locaux ou à distance, doivent disposer d’une banque de mots de passe qui peut être compromise.

La banque de mots de passe de l’administrateur de mots de passe doit être efficacement cryptée et l’accès strictement contrôlé. Grâce aux applications téléphoniques mobiles et aux interfaces Web, les administrateurs de mots de passe sur le cloud fournissent un accès permanent à ses utilisateurs, à tout moment.

LastPass est un administrateur de mots de passe populaire.

Créez un compte d’essai LastPass :

* + 1. Ouvrez un navigateur Web et accédez à l’adresse <https://lastpass.com/>.
    2. Cliquez sur **Essai gratuit** pour créer un compte d’essai.
    3. Remplissez les champs, selon les instructions.
    4. Définissez un mot de passe principal. Ce mot de passe vous permettra d’accéder à votre compte LastPass.
    5. Téléchargez et installez le client LastPass adapté à votre système d’exploitation.
    6. Ouvrez le client et connectez-vous avec votre mot de passe principal LastPass.
    7. Explorez l’administrateur de mots de passe LastPass.

Lorsque vous ajoutez des mots de passe dans LastPass, où ces derniers sont-ils stockés ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Les mots de passe sont stockés dans le cloud, sur les serveurs de LastPass.

À part vous, au moins une entité tierce a accès à vos mots de passe. Qui est cette entité ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

LastPass

Même si stocker tous vos mots de passe au même emplacement peut être pratique, cela présente des risques. Pouvez-vous donner un exemple ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Plusieurs réponses sont possibles. Les serveurs de LastPass deviennent une cible importante pour les agresseurs, car ils contiennent les mots de passe de nombreux utilisateurs. La responsabilité de conserver vos mots de passe a maintenant été déléguée à une entreprise tierce et vous n’avez pas de contrôle sur leurs politiques de sécurité. Vous choisissez d’avoir confiance en leur capacité à protéger vos mots de passe, mais rien ne la garantit.

1. Qu’est-ce qu’un mot de passe fiable, alors ?

Choisissez un mot de passe facile à se rappeler, mais difficile à déchiffrer, grâce aux caractéristiques de mot de passe fiable indiquées au début de cet atelier. Les mots de passe complexes sont acceptables, tant qu’ils ne contredisent des critères plus importants comme la simplicité de leur mémorisation.

En cas d’utilisation d’un administrateur de mots de passe, nul besoin d’une simplicité de mémorisation.

Voici une brève récapitulation :

Choisissez un mot de passe dont vous pouvez vous rappeler.

Choisissez un mot de passe auquel une personne tierce ne peut vous associer.

Choisissez des mots de passe différents et n’utilisez jamais le même pour des services différents.

Les mots de passe complexes sont acceptables, tant qu’ils ne sont pas difficiles à se rappeler.