Guide des bonnes pratiques pour les mots de passe

La sécurité de vos informations personnelles et professionnelles dépend en grande partie de la robustesse de vos mots de passe. Pour vous accompagner dans cette démarche, nous avons mis à jour nos recommandations en accord avec les dernières directives de la Commission nationale de l'informatique et des libertés (CNIL) et de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

1. Authentification à Plusieurs Facteurs (MFA)

Utilisez l'authentification à plusieurs facteurs (MFA) chaque fois que cela est possible. Cela offre une couche supplémentaire de sécurité en demandant une preuve d'identité au-delà du simple mot de passe.

2. Évaluation des Risques

Considérez les facteurs de risque suivants lors de la création et de la gestion de vos mots de passe :

- Simplicité du mot de passe

- Risque d'écoute sur le réseau

- Conservation en clair du mot de passe

- Faiblesse des modalités de renouvellement du mot de passe pour les postes à droits élevés

3. Complexité et Longueur

Suivez les recommandations de la CNIL et de l'ANSSI en matière de complexité et de longueur des mots de passe. Par exemple :

- Exemple 1 : Au moins 12 caractères incluant majuscules, minuscules, chiffres, et caractères spéciaux à choisir dans une liste d'au moins 37 caractères spéciaux possibles.

- Exemple 2 : Au moins 14 caractères incluant majuscules, minuscules et chiffres (sans caractère spécial obligatoire).

- Exemple 3 : Utilisez une phrase de passe composée d'au minimum 7 mots.

4. Entropie

Comprenez le concept d'entropie pour évaluer la robustesse de vos mots de passe. L'entropie mesure le degré d'imprédictibilité théorique et la capacité de résistance à une attaque par force brute.

- Utilisez l'outil en ligne Howsecureismypassword si vous voulez vous faire une idée :

https://howsecureismypassword.net/

5. Renouvellement de Mot de Passe

Pour les utilisateurs classiques, concevez un mot de passe robuste et ne le changez que si nécessaire. Cependant, les utilisateurs privilégiés doivent renouveler leurs mots de passe à intervalles réguliers définis à 90 jours.

6. Utilisation de Gestionnaires de Mots de Passe

Recourez à des gestionnaires de mots de passe fiables pour générer et stocker en toute sécurité des mots de passe complexes.

7. Éviter l'Évidence

N'élaborez pas des mots de passe basés sur des informations évidentes telles que votre nom, date de naissance, ou d'autres données facilement accessibles.

Sources et Outils Recommandés

- [Nouvelles recommandations sur les mots de passe - CNIL] (https://www.cnil.fr/fr/nouvelles-recommandations-sur-les-mots-de-passe)

- [Recommandations relatives à l'authentification multi facteur et aux mots de passe - ANSSI] (https://www.ssi.gouv.fr/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/)

Pour vous aider dans la compréhension de ces règles, consultez les outils recommandés par la CNIL et l'ANSSI.

Recommandations pour le changement du parc informatique du 10 janvier 2024.

Chères utilisatrices, chers utilisateurs,

Nous sommes ravis de vous annoncer que le 10 janvier 2024, vos nouveaux ordinateurs portables feront leur entrée, apportant avec eux une expérience informatique améliorée. Pour vous accompagner dans cette transition en douceur, nous partageons avec enthousiasme les conseils de la CNIL pour des mots de passe robustes :

Longueur et Complexité : Utilisez des mots de passe d'au moins 12 caractères avec une combinaison de majuscules, minuscules, chiffres et caractères spéciaux.

Évitez les Informations Faciles : N'utilisez pas d'informations facilement devinables, comme votre nom ou votre date de naissance.

Unicité des Mots de Passe : Utilisez des mots de passe différents pour chaque compte en ligne pour éviter les impacts en cas de compromission.

Évitez les Mots Courants : Évitez les mots courants du dictionnaire pour contrer les attaques de force brute.

Renouvellement et Gestion : Conservez un mot de passe robuste sans renouvellement périodique. Utilisez un gestionnaire de mot de passe fiable comme Keepass ou Bitwarden. Un gestionnaire de mots de passe est un outil qui stocke de manière sécurisée et organise les mots de passe que vous utilisez pour accéder à vos comptes en ligne.

Phrases de Passe : Préférez les phrases de passe pour une mémorisation facilitée et une complexité accrue.

Authentification à Deux Facteurs : L'authentification à deux facteurs (2FA) pour une sécurité renforcée. Ceci est obligatoire sur votre poste et sur vos mails pour le moment, d’autres

Précautions Générales : Ne partagez jamais vos mots de passe et évitez de les enregistrer dans des endroits non sécurisés.

Outils en Ligne : Utilisez des outils en ligne tels que HowSecureIsMyPassword pour évaluer et générer des mots de passe sécurisés.

N’hésitez pas à consulter notre guide sur la bonne gestion de mots de passes. Ce guide se trouve en pièce jointe, ainsi que le planning de distribution des postes. Soyez prêts à explorer de nouvelles possibilités et à renforcer ensemble la sécurité de notre environnement informatique. Nous sommes là pour vous, à chaque étape de ce passionnant voyage numérique