



Lorsque vous allumez votre ordinateur, il vous est demandé un mot de passe pour ouvrir votre session Windows.

Ce mot de passe peut être comparé à la **clé de votre maison**. Tout comme la clé vous permet d'entrer chez vous et d'accéder à votre espace personnel, le mot de passe de session est la clé virtuelle qui vous ouvre les portes de votre environnement de travail (messagerie, dossiers confidentiels, applications métiers, ...).

Il sécurise l'accès à votre ordinateur et constitue la première ligne de défense pour protéger vos informations confidentielles.

De la même manière que vous choisissez une clé solide et unique pour protéger votre maison, il est essentiel de créer un mot de passe robuste et unique pour préserver la sécurité de votre poste de travail, et **par extension, la sécurité du réseau informatique du Département**.

Cette fiche vous donnera quelques astuces et règles d'or pour renforcer votre mot de passe. Elle sera amenée à évoluer suivant les nouvelles indications de sécurisation des systèmes d'information.

LE SAVIEZ-VOUS ?

Un mot de passe complexe peut être craqué en plusieurs années contre quelques secondes pour un mot de passe composé seulement que de chiffres. (voir ci-joint le Tableau de complexité des mots de passe et temps de décryptage)

5 RÈGLES D'OR POUR UN MOT DE PASSE SÉCURISÉ

1 | Tu ne partageras point

Un mot de passe c'est comme une brosse à dents, ça ne se partage pas ! Il est strictement personnel et ne doit être divulgué à personne : collègues (y compris de la DSIAN), famille, amis...

2 | Tu ne le noteras point

Noter son mot de passe sur un post-it collé à l'écran d'ordinateur ou sous le clavier est une pratique à proscrire. Pour vous aider à retenir votre mot de passe, vous pouvez utiliser des moyens mnémotechniques :

- Méthode des premières lettres d'une phrase facile à retenir : « Ma voisine a 2 chiens adorables qui s'appellent Max et Bella » > « Mva2caqs'aM&B »

- Méthode phonétique : « j'ai acheté huit CD pour cent euros cet après-midi » > « Ght8CD%E7am »

- Vous pouvez également inventer votre propre méthode !

3 | Un mot de passe unique pour ta session Windows tu auras

Utiliser le même mot de passe pour plusieurs comptes simplifie considérablement la tâche des pirates informatiques : ce mot de passe unique lui permettra d'accéder à tous vos comptes et augmentera donc le risque de compromission globale.

4 | Complexifier ton mot de passe tu sauras

Une technique d'attaque répandue, dite par « force brute », consiste à essayer toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de passe. Réalisées par des ordinateurs, ces attaques peuvent tester des dizaines de milliers de combinaisons par seconde. Pour empêcher ce type d'attaque, votre mot de passe doit être :

- LONG et COMPLEXE : Je crée un mot de passe contenant 12 caractères au minimum et en utilisant 3 types de caractères différents (minuscule, majuscule, chiffre, caractère spécial ?\$&\$€@!.*)

- IMPOSSIBLE A DEVINER : Mon mot de passe ne doit avoir aucun lien avec des informations personnelles (ex. : date de naissance de mes enfants, nom de mon chien, de ma ville ou de mon chanteur préféré...). J'évite également les suites logiques du type «azerty», «12345», «abcdef»...



5 | Changer de mot de passe de session tous les 6 mois tu devras

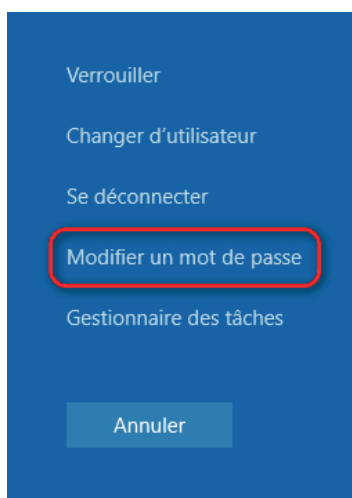
Afin de réduire les risques de cyberattaque, vous devez changer votre mot de passe de session Windows tous les 6 mois.

Changer son mot de passe de session Windows :

1 Appuyez simultanément sur les touches



2 Sélectionnez « Modifier un mot de passe »



3 Modifiez votre mot de passe



Quels sont les impacts sur les applications que j'utilise ?

Dans l'éventail d'applications que vous utilisez au quotidien, certaines seront impactées par le changement du mot de passe de session Windows. Il vous faudra retaper le même mot de passe pour ces applications :

- ASTRE
- HORUS
- CHRONOTIME
- GED Social
- SEDIT RH
- AIRS Courrier
- GECCO
- GED MDPH

... et sur mon smartphone ?

Pour vous connecter à votre messagerie Outlook, le nouveau mot de passe doit être renseigné sur votre smartphone professionnel. Un tutoriel est disponible ci-joint pour vous aider à effectuer la démarche. Si besoin, contactez la hotline DSIAN.

J'ai oublié mon mot de passe...

Si vous ne vous souvenez plus de votre mot de passe, au bout de 3 tentatives infructueuses votre session sera bloquée. Il vous faudra contacter la hotline de la DSIAN pour la réactiver.

IMPORTANT

Un mot de passe complexe ne sert à rien si vous ne verrouillez pas votre session Windows lorsque vous quittez votre poste de travail, même pour quelques minutes !

Pour cela appuyez sur les touches de raccourci :

