

# LES FICHES OUI INFORMATIQUE



**La gestion des mots de passe est cruciale pour assurer la sécurité de vos comptes en ligne et de vos données personnelles.**

**Voici quelques conseils pratiques pour une gestion efficace des mots de passe.**

## Retour sur les Mots de Passe

### Complexité des mots de passe

Utilisez des mots de passe complexes qui combinent des lettres majuscules et minuscules, des chiffres et des caractères spéciaux. Évitez les mots de passe évidents comme **123456** ou **motde-passe**.

### Longueur des mots de passe

Optez pour des mots de passe longs. Plus un mot de passe est long, plus il est difficile à pirater. Essayez d'utiliser au moins 10 à 12 caractères.

### Éviter les informations personnelles

Évitez d'inclure des informations personnelles évidentes, telles que votre nom, date de naissance ou d'autres détails facilement accessibles ou devinables.

### Utiliser des phrases de passe

Créez des phrases de passe en combinant des mots, des chiffres et des caractères spéciaux. Ces phrases peuvent être plus faciles à retenir tout en étant sécurisées.

Par exemple :

**1BonMot2Passe\$**

**1PetitChien&&**

### Mots de passe uniques pour chaque compte

N'utilisez pas le même mot de passe pour plusieurs comptes. Si un mot de passe est compromis, cela ne mettra pas en danger vos autres comptes.

### Gestion avec un gestionnaire de mots de passe

Utilisez un gestionnaire de mots de passe pour stocker en toute sécurité et générer des mots de passe complexes. Ces outils simplifient la gestion des nombreux mots de passe que vous pouvez avoir.

### Changement régulier des mots de passe

Changez vos mots de passe régulièrement. Si un compte est compromis, changer le mot de passe réduit les risques.

### Vérification des comptes compromis

Utilisez des services en ligne qui vous permettent de vérifier si vos comptes ont été compromis dans des violations de données. Cela peut vous alerter sur la nécessité de changer vos mots de passe.

Password:

\*\*\*\*\*

### Authentification à deux facteurs (2FA)

Activez l'authentification à deux facteurs chaque fois que possible. Cela ajoute une couche de sécurité en demandant une deuxième forme d'identification, comme un code envoyé sur votre téléphone.

## Bien appréhender les mots de passe

### Éviter de sauvegarder les mots de passe dans le navigateur

Bien que les navigateurs proposent souvent de sauvegarder les mots de passe, il est plus sûr d'utiliser un gestionnaire de mots de passe dédié. Cela réduit le risque en cas d'accès non autorisé à votre ordinateur.

### Partager les mots de passe avec prudence

Si vous devez partager un mot de passe, assurez-vous de le faire de manière sécurisée et uniquement avec des personnes de confiance. Évitez les communications non sécurisées comme les emails non chiffrés.

## OUI Informatique

18 boulevard de la capelle

12100 MILLAU

05 65 46 31 84 – 07 87 09 00 51

[contact@oui-informatique.fr](mailto:contact@oui-informatique.fr)

[www.oui-informatique.fr](http://www.oui-informatique.fr)



En suivant ces conseils, vous renforcez la sécurité de vos comptes en ligne et minimisez les risques de compromission de données.

La gestion des mots de passe est un aspect essentiel de la sécurité informatique personnelle.

**En cas de doutes, contactez-nous !**