



Comment choisir un bon mot de passe lorsque vous créez un compte sur Internet ?



Publié le 6 mai 2021

[comment gérer ses mots de passe](#)

[gérer ses mots de passe](#)

[mots de passe](#)

 16042 Temps de lecture : 18 min

Que ce soit pour regarder un film sur une plateforme de vidéo en streaming, réserver une semaine de vacances ou payer vos impôts, créer un compte sur Internet est désormais une pratique à laquelle vous pouvez difficilement échapper. Une démarche qui nécessite obligatoirement de définir un nouveau **mot de passe** afin de protéger vos informations personnelles. Pour sécuriser vos comptes, mieux vaut donc choisir des codes d'accès solides et complexes à deviner. Pour la journée mondiale du mot de passe, [Cybermalveillance.gouv.fr](https://www.cybermalveillance.gouv.fr) vous donne les clés pour choisir un bon mot de passe pour vos comptes Internet.

L'affichage du contenu tiers "dailymotion" a été bloqué conformément à vos préférences.

Messageries, [réseaux sociaux](#), banques... Désormais, la plupart des services en ligne vous invitent à créer un compte personnalisé. Pour cela, il vous est demandé de compléter certaines informations – nom, prénom, adresse de messagerie, identifiant... – et de définir un nouveau mot de passe (*password* en anglais). Il s'agit de la clé d'accès numérique qui vous permettra de vous authentifier à chaque fois que vous souhaiterez vous connecter à votre compte et protéger les informations qui y sont entreposées.

Étant donné le grand nombre de mots de passe à créer, il est souvent tentant d'opter pour la solution de facilité : choisir un mot de passe générique de type "123456", utiliser le même code personnel pour tous vos comptes Internet ou utiliser un mot de passe basé sur une information personnelle (date de naissance, prénom d'un enfant, etc.). Des clés d'accès souvent très « simples » à deviner pour les cybercriminels qui chercheraient à pirater votre compte.

[Pour naviguer d'une manière plus sécurisée sur Internet](#), nous vous conseillons de respecter quelques consignes de sécurité élémentaires.

1. Quelles sont les bonnes pratiques générales à appliquer ?

1. Utiliser un mot de passe différent pour chaque accès

Face au nombre de comptes que nous sommes amenés à créer, il est tentant, pour s'y retrouver, d'utiliser à chaque fois le même **mot de passe**. Si une personne malintentionnée découvre ce mot de passe, elle pourra alors accéder à l'ensemble de vos données !

La plupart de services étant aujourd'hui dématérialisés, les données que vous renseignez sur vos différents comptes sont souvent importantes et **sensibles** :

- Identité
- Numéros de carte bancaire
- Numéros de téléphone
- Adresse
- Emails
- Etc.

Nous vous recommandons donc de **choisir un mot de passe différent pour chaque compte**.

2. Choisir un mot de passe robuste

Votre mot de passe doit être **complexe**, afin que personne ne puisse le deviner, pas même votre famille ou votre entourage. Il doit comporter au minimum 8 à 12 caractères mélangeant les majuscules, les minuscules, des chiffres et des caractères spéciaux.

Lorsque vous choisissez votre mot de passe, évitez donc toutes les informations qui vous concernent et qui sont facilement accessibles (sur vos réseaux sociaux par exemple) :

- Dates de naissance de vos proches
- Noms de vos proches
- Noms de vos animaux de compagnie
- Etc.

3. Changer votre mot de passe au moindre doute

Dans le cadre de votre navigation personnelle, modifiez votre mot de passe au moindre soupçon d'utilisation frauduleuse, comme par exemple une activité inhabituelle de ce compte ou si vous avez entendu parler d'un piratage d'un service que vous utilisez.

Dans un contexte professionnel, veillez à renouveler vos mots de passe de façon régulière et systématique, même si vous êtes vigilant et ne soupçonnez aucune fraude ! Vous pouvez par exemple décider de les changer dès à présent, puis tous les deux ou trois mois.

4. Garder ses mots de passe pour soi

Ne communiquez jamais **votre mot de passe** à une personne de votre entourage, quelle qu'elle soit. L'idée n'est pas d'être méfiant à outrance mais de rester vigilant : les enjeux sont tels que votre mot de passe doit rester totalement **confidentiel**. Jamais aucune entreprise ou service d'État ne vous le demandera par téléphone ou par courriel. Si vous recevez une telle sollicitation, c'est qu'il s'agit d'une tentative d'arnaque par [hameçonnage](#).

Veillez également à faire preuve de vigilance concernant les informations que vous pouvez laisser traîner. S'il est tentant d'écrire certains codes sur un bout de papier – celui de l'accès au WIFI de votre box internet, par exemple – n'écrivez jamais **vos mots de passe personnels ou professionnels**.

5. N'utilisez pas vos mots de passe sur un ordinateur partagé

Les ordinateurs en libre accès peuvent être piégés ou contrôlés par des cybercriminels dans le but de vous dérober des informations personnelles sensibles (mots de passe, données bancaires, identité, etc...).

Si vous êtes obligés d'utiliser un ordinateur partagé, utilisez le mode "navigation privée", n'enregistrez jamais vos mots de passe dans le navigateur et fermez vos sessions après utilisation.

Enfin, dès que vous accédez à un ordinateur de confiance, n'hésitez pas à modifier tous les mots que vous avez utilisés sur l'ordinateur partagé.

6. Changez les mots de passe par défaut des services que vous utilisez

De nombreux équipements tels que les objets connectés ou des services proposent des mots de passe par défaut qui ne sont parfois pas assez complexes. Par ailleurs, ces mots de passe par défaut sont souvent connus des cybercriminels. Il est donc essentiel de les modifier au plus vite par vos propres mots de passe.

7. Choisissez un mot de passe particulièrement complexe pour votre boîte de messagerie

L'affichage du contenu tiers "dailymotion" a été bloqué conformément à vos préférences.

AUTORISER LES CONTENUS DAILYMOTION

Votre adresse de messagerie est souvent associée à un grand nombre de vos services en ligne (réseaux sociaux, sites de banques, commerces en ligne, etc.) sur laquelle vous pouvez demander à recevoir les liens de réinitialisation des mots de passe de ces services.

Si votre messagerie est piratée par un cybercriminel, il pourrait utiliser la fonctionnalité “mot de passe oublié” des différents sites auxquels vous pouvez accéder pour en prendre le contrôle. Votre boîte de messagerie est donc un élément majeur de votre sécurité numérique et la plus importante à sécuriser.

2. Comment créer un mot de passe sécurisé ?

Si vous suivez bien ces différentes recommandations, vous devriez avoir de nombreux nouveaux mots de passe à (re)définir. Comment procéder de manière simple ?

Deux options s'offrent à vous :

1. Créer soi-même son mot de passe

Si vous choisissez cette option, faites preuve d'inventivité ! Votre **mot de passe** doit être suffisamment long et complexe en intégrant des lettres (majuscules et minuscules), des chiffres, de la ponctuation, des caractères spéciaux et n'avoir aucun rapport avec votre vie personnelle.

Pour mieux vous en souvenir, différentes méthodes existent. Vous pouvez par exemple pour créer des mots de passe :

- Retenir la ou les premières lettres de chaque mot composant une phrase
- Utiliser la phonétique d'une phrase pour créer une suite de lettres et de chiffres correspondant
- Créer une méthode connue de vous seul

Ainsi, vos différents mots de passe seront plus **faciles à mémoriser**.

Un inconvénient cependant : cette méthode est celle qui vous demandera le plus de temps et d'imagination.

2. Utiliser un générateur de mots de passe

Créer vous-même vos mots de passe complexes vous paraît laborieux ? Nous vous recommandons d'**utiliser un générateur de mots de passe** qui se chargera de les inventer pour vous.

Le gestionnaire de mots de passe **KeePass**, logiciel gratuit et certifié par l'**Agence Nationale de la Sécurité des Systèmes d'Information** (ANSSI), propose une fonctionnalité de génération de mots de passe complexes et aléatoires. Avec cette méthode, vos mots de passe **générés automatiquement** seront ainsi **très robustes**.

Il faut noter que les codes d'accès proposés ne répondront à aucune logique particulière : ils seront alors **plus compliqués à mémoriser** que ceux que vous imaginerez vous-mêmes. C'est pourquoi KeePass dispose également d'une fonction qui permet de stocker vos mots de passe en toute sécurité.

3. À quoi sert un gestionnaire de mots de passe ?

L'affichage du contenu tiers "dailymotion" a été bloqué conformément à vos préférences.

AUTORISER LES CONTENUS DAILYMOTION

Une fois que vous avez défini vos différents mots de passe, il faut tous les mémoriser, ce qui n'est pas toujours simple. En effet, qui n'a jamais douté ou oublié un mot de passe ?

Pour ne pas avoir à demander un nouveau mot de passe à chaque oubli, **le gestionnaire de mots de passe** se charge de tout mémoriser pour vous. Très simple d'utilisation, il vous permet d'avoir accès à tout moment à l'ensemble de vos codes d'accès.

Quel outil choisir ?

Attention ! En naviguant sur internet à la recherche d'un outil, de nombreux gestionnaires vous sont proposés. Nous vous recommandons fortement d'utiliser l'outil KeePass, seul gestionnaire français gratuit qui soit certifié par l'ANSSI.

4. Quelques pratiques avancées pour sécuriser ses mots de passe...

1. Autoriser la double authentification

L'affichage du contenu tiers "dailymotion" a été bloqué conformément à vos préférences.

Afin de protéger vos données personnelles et naviguer sur Internet en toute sécurité, **la double authentification** – parfois également appelée « authentification à double facteur » ou 2FA (pour *two-factor authentication* en anglais) – fait partie des bonnes pratiques à mettre en place.

Exemples non exhaustifs de services répandus proposant la double authentification :

- Gmail, Outlook, Yahoo Mail...
- Facebook, Instagram, LinkedIn, Twitter...
- Skype, WhatsApp...
- Amazon, eBay, Paypal...
- Apple iCloud, Dropbox, Google Drive, One Drive...

Comment cela fonctionne ?

En plus de vous demander de renseigner les informations classiques liées à votre compte – **identifiant et mot de passe** – le service se charge de vérifier que vous êtes bien en possession d'un téléphone ou autre équipement si un nouvel appareil inconnu tente de se connecter à votre compte. Cela peut prendre la forme d'un code provisoire que vous pouvez recevoir, par exemple, par SMS sur votre téléphone mobile ou qui peut être généré par une application ou une clé spécifique que vous contrôlez.

2. Tester la robustesse de ses mots de passe

Par ailleurs, n'hésitez pas à tester la robustesse de vos mots de passe. Également proposée par l'outil KeePass, cette fonctionnalité vous donnera une idée du **niveau de protection** de vos comptes.

Pour aller plus loin :



Les mots de passe

Retrouvez les 10 bonnes pratiques à adopter pour gérer efficacement vos mots de passe.

Publié le 08/04/2021
PDF 311 Ko

TÉLÉCHARGER [↓](#)



Les mots de passe en fiche mémo

Apprenez rapidement à gérer vos mots de passe grâce à notre fiche mémo.

Publié le 08/04/2021

PDF 185 Ko

[TÉLÉCHARGER](#) 

A LIRE AUSSI



Pourquoi et comment bien gérer ses mots de passe ?

[Lire la bonne pratique](#)

INSCRIVEZ-VOUS À LA NEWSLETTER

Tenez-vous informé(e) de l'actualité de la cybermalveillance et des nouvelles menaces

Entrez votre adresse email



OK



À PROPOS

[Qui sommes-nous ?](#)

[Mentions légales](#)

[Politique de confidentialité](#)

DIVERS

[Plan du site](#)

[Presse](#)

[Marchés publics](#)

[Label ExpertCyber](#)

NOUS SUIVRE



GOUVERNEMENT.FR 

SERVICE PUBLIC 

FRANCE.FR 

ELYSEE.FR 

LEGIFRANCE 

DATA.GOUV.FR 