RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

mémo

10 CONSEILS POUR GÉRER VOS MOTS DE PASSE

1. Utilisez un mot de passe différent pour chaque service
2. Utilisez un mot de passe suffisamment long et complexe
3. Utilisez un mot de passe impossible à deviner
4. Utilisez un gestionnaire de mots de passe
5. Changez votre mot de passe au moindre soupçon
6. Ne communiquez jamais votre mot de passe à un tiers
7. N'utilisez pas vos mots de passe sur un ordinateur partagé
8. Activez la double authentification lorsque c'est possible
9. Changez les mots de passe par défaut des différents services auxquels vous accédez
10. Choisissez un mot de passe particulièrement robuste pour votre messagerie

Pour en savoir plus ou vous faire assister, rendez-vous sur Cybermalveillance.gouv.fr

ADOPTER LES BONNES PRATIQUES

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

DISPOSITIF NATIONAL CYBERMALVEILLANCE.GOUV.FR

SES MISSIONS

1. **ASSISTANCE AUX VICTIMES** D'ACTES DE CYBERMALVEILLANCE
2. **INFORMATION ET SENSIBILISATION** SUR LA SÉCURITÉ NUMÉRIQUE
3. **OBSERVATION ET ANTICIPATION** DU RISQUE NUMÉRIQUE

QUI EST CONCERNÉ ?

RETROUVEZ TOUTES NOS PUBLICATIONS SUR:
www.cybermalveillance.gouv.fr

Version 3.0

sécurité en ligne

créer un mot de passe sécurisé

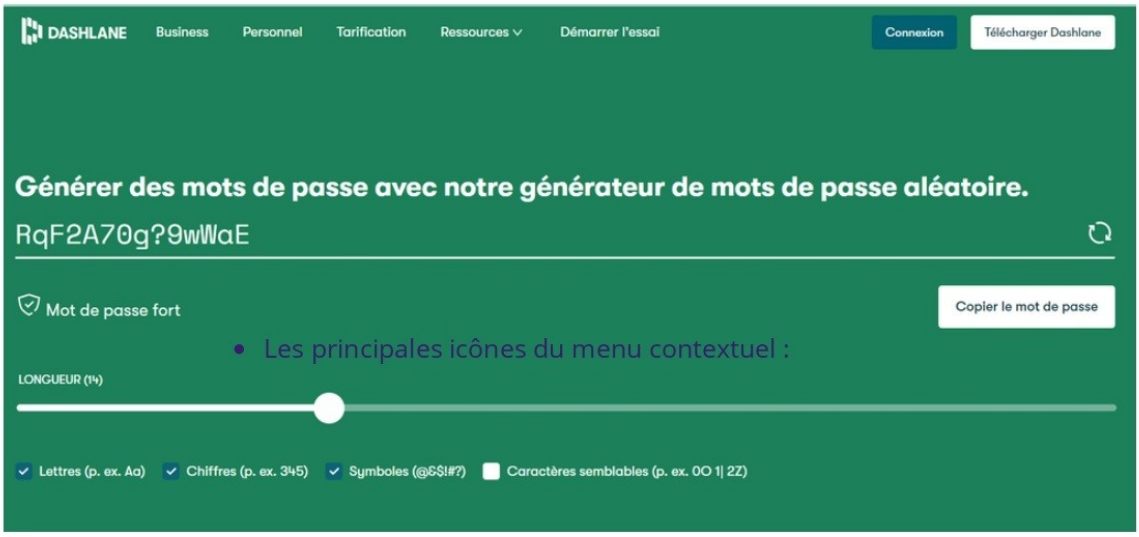
Créer un mot de passe sécurisé

Un mot de passe doit être **fort,** c'est à dire qu'il doit être suffisamment long et compliqué pour ne pas être piraté.

Pour être fort et sécurisé, il doit :

- ne contenir aucune donnée personnelle (pas de prénom, de lieu de résidence ou de naissance, pas de date de naissance, pas les prénoms des enfants ou conjoints…
- il doit être différent sur chaque site web
- il doit être composé d'un minimum de 9 caractères, de préférence avec des minuscules, des majuscules, des chiffres et des symboles
- idéalement être changé régulièrement

Vous pouvez vous servir d'un générateur de mot de passe tel que celui-ci : https://www.dashlane.com/fr/features/password-generator



- Les principales icônes du menu contextuel :

Le mot de passe de votre messagerie habituelle doit être particulièrement robuste car il est la clé d'accès à tous vos comptes en ligne.
Depuis votre messagerie, il est possible de changer absolument tous vos autres mots de passe.
Utilisez la double authentification sur tous vos sites dès que vous en avez la possibilité

Générateur de mot de passe gratuit :
https://www.dashlane.com/fr/features/password-generator

sécurité en ligne

créer un mot de passe sécurisé

Créer un mot de passe sécurisé

A titre informatif, un mot de passe peut être piraté très rapidementt selon le nombre de caractères et la complexité de celui-ci :

COMBIEN DE TEMPS FAUT-IL À UN PIRATE POUR TROUVER VOTRE MOT DE PASSE 2024

www.hivesystems.com/password

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minescules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Immédiat	Immédiat	3 secs	6 secs	9 secs
5	Immédiat	4 secs	2 mins	6 mins	10 mins
6	Immédiat	2 mins	2 heures	6 heures	12 heures
7	4 secs	50 mins	4 jours	2 semaines	1 mois
8	37 secs	22 heures	8 mois	3 ans	7 ans
9	6 mins	3 semaines	33 ans	161 ans	479 ans
10	1 heure	2 ans	1k ans	9k ans	33k ans
11	10 heures	44 ans	89k ans	618k ans	2M ans
12	4 jours	1k ans	4M ans	38M ans	164M ans
13	1 mois	29k ans	241M ans	2Md ans	11Md ans
14	1 an	766k ans	12Md ans	147Md ans	805Md ans
15	12 ans	19M ans	652Md ans	9Bn ans	56Bn ans
16	119 ans	517M ans	33Bn ans	566Bn ans	3qd ans
17	1k ans	13Md ans	1qd ans	35qd ans	276qd ans
18	11k ans	350Md ans	91qd ans	2qn ans	19qn ans

Si vous avez le moindre doute concernant une éventuelle fuite de vos mots de passe, changez -les **immédiatement.**

Vous pouvez vérifier sur ce site si certains de vos comptes en ligne utilisant votre adresse mail ont pu être piratés, si c'est le cas modifiez vos mots de passe sur les sites concernés **https://haveibeenpwned.com/**

Double authentification

Qu'est-ce que la double authentification ?

La double authentification, aussi appelée validation ou vérification en 2 étapes est une fonctionnalité qui permet de renforcer la sécurité de vos comptes afin d'éviter leur piratage en agissant comme une protection supplémentaire en cas de vol de votre mot de passe.
La double authentification peut s'activer sur de nombreux services en ligne, comme votre compte de messagerie, sur les réseaux sociaux et même sur certains sites de vente en ligne…

Comment fonctionne la double authentification ?

Une fois que vous avez activé la double authentification, en plus de votre nom de compte et de votre mot de passe, ces services vous demanderont une confirmation en fournissant un code provisoire reçu par SMS ou par message (mail), via une application ou une clé spécifique dont vous disposez, ou encore par reconnaissance biométrique.
En fonction du service, cette demande de confirmation pourra vous être demandée à la première connexion ou à chaque connexion, à intervalle régulier, mais surtout à chaque fois qu'un nouvel équipement inconnu par le service concerné tentera de se connecter à votre compte.
Vous seul pourrez donc autoriser un nouvel appareil à se connecter à vos comptes protégés par la double authentification.

À quoi ça sert la double authentification ?

À bloquer toute tentative d'accès à votre compte, à votre insu, avec votre mot de passe.
Dans ce cas, si une personne malveillante essayait d'accéder à votre compte avec votre mot de passe, elle en serait empêchée et vous recevriez une alerte vous notifiant que quelqu'un a essayé de s'y connecter.
Il faudra alors changer de mot de passe immédiatement pour bloquer une éventuelle tentative de connexion et de piratage de votre compte.