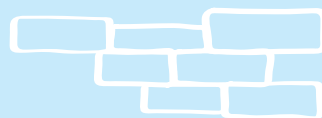


Comment créer un mot de passe sûr ?

- Utilisez une phrase de passe que vous pourriez facilement mémoriser.
M4myF4itDesCrepesLeDim4nche!
- Utilisez un mot de passe différent pour chaque profil. Moins de répétitions = moins de risques.
- Appliquez un verrouillage supplémentaire à tous vos comptes importants. Configurez le 2FA pour vos e-mails, Facebook, les boutiques en ligne.
- Conservez vos mots de passe en lieu sûr. Utilisez un carnet ou un gestionnaire de mots de passe.
- Ne partagez en aucun cas vos mots de passe avec d'autres personnes. Pas même avec des personnes en qui vous faites absolument confiance.
- Osez demander de l'aide. À des amis et à des membres de la famille ou consultez le site tousconnectéstousprotégés.be.



Tous connectés, tous protégés

Tous connectés tous protégés est une initiative de DNS Belgium qui veut aider les gens à se protéger mutuellement contre les escroqueries en ligne.

L'internet en toute sécurité, cela ne se fait pas tout seul. La famille, les amis ou les voisins peuvent vous aider à garder un œil sur ce qui se passe. Avec des conseils, des informations et des histoires, nous vous aidons, vous et votre entourage, à créer des mots de passe sûrs.

Plus d'informations ?

www.tousconnectéstousprotégés.be

dnsbelgium

tous
connectés,
tous
protégés

Estceunmotdep4ssesécurisé?

Pas à pas

Comment créer des mots de passe sûrs ?

3 conseils pour créer des mots de passe qui vous protègent contre la fraude.



dnsbelgium

Quand un mot de passe est-il sûr ?

- Utilisez au moins 15 caractères
- Combinez des lettres, des chiffres et des symboles
- Et utilisez un mot de passe différent pour chaque compte

Renforcer la sécurité de vos mots de passe ?

Avec une authentification à deux facteurs (2FA), vous ajoutez un verrouillage supplémentaire à votre compte : en plus de votre mot de passe, vous devrez fournir une seconde confirmation (par SMS, empreinte digitale ou reconnaissance faciale).

Même si quelqu'un connaît votre mot de passe, votre compte reste sécurisé.

Comment configurer :

1. Sélectionnez vos comptes les plus importants (p.ex., e-mail, Facebook).
2. Dans les paramètres, allez dans « Sécurité » ou « Vérification en deux étapes ».
3. Choisissez votre mode de confirmation: par SMS, empreinte digitale ou reconnaissance faciale.
4. Suivez les étapes indiquées à l'écran.

Utiliser des mots de passe sûrs ? Voici comment procéder :

Ces 3 conseils vous aideront à créer des mots de passe sûrs pour tous vos profils.

1. Ajoutez un verrouillage supplémentaire à vos comptes

Un verrouillage supplémentaire ? Il s'agit d'authentification à deux facteurs ou 2FA et cela fonctionne comme votre application bancaire ou itsme.

1. Vous vous connectez avec votre mot de passe
2. Vous recevez un code sur votre GSM (ou vous confirmez avec votre empreinte digitale ou avec la fonction de reconnaissance faciale)
3. Vous saisissez ce code et vous seul(e) pouvez accéder à votre compte

2. Créez une phrase de passe

Un bon mot de passe est **long et personnel**.

Pensez à une phrase qui a du sens pour vous.

Par exemple :

- MonChienFri pouilleAboie2025!
- M4myF4itDesCrepesLeDim4nche!

Important : veillez aussi à inclure des chiffres et des caractères spéciaux.

tous
connectés,
tous
protégés



3. Protégez vos mots de passe

- Notez vos mots de passe dans un carnet (et conservez-le en lieu sûr, loin de votre ordinateur)
- Ou utilisez un **gestionnaire de mots de passe**, étant donné que cet outil :
 - crée des mots de passe sécurisés pour vous,
 - les conserve en toute sécurité,
 - et les saisit automatiquement lorsque vous vous connectez.

C'est pratique : vous n'avez à mémoriser qu'un seul mot de passe

Des gestionnaires fiables :
Bitwarden, 1Password, Dashlane

Besoin d'aide ?

Demandez à un membre de la famille, à un ami ou à un voisin de vous aider.

Ou consultez le site

www.tousconnectéstousprotégés.be

