Mot de passe

Les mots de passe sont essentiels

Les mots de passe restent encore le moyen principal aujourd'hui pour contrôler l'accès à vos informations essentielles et en particulier à l'ensemble de vos comptes en ligne : courrier électronique, réseaux sociaux, banque en ligne ; ils vous sont aussi confiés pour accéder à des ressources professionnelles.

Parfois l'accès à un compte pourra être détourné pour faciliter l'accès à d'autres comptes. Ainsi, votre adresse de courrier électronique permet parfois de recevoir des liens de renouvellement de mots de passe pour d'autres services.

Enfin, les services que vous utilisez relaient votre image : si quelqu'un prend le contrôle de votre adresse de courrier électronique et de vos comptes de réseaux sociaux, il peut avoir accès à vos listes de contacts et s'adresser à vos amis comme si c'était vous. C'est une technique couramment utilisée par des escrocs sur Internet.

Pour toutes ces raisons, **il est indispensable de maîtriser et sécuriser l'usage de vos mots de passe**. Les quelques conseils simples qui suivent vous y aideront.

D'autres ressources sont disponibles sur la page de **notre campagne « Semaine du mot de passe »** https://www.cyberprevention.fr/campagnes/semaine-du-mot-de-passe/ .

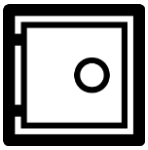
Conseils simples pour sécuriser vos mots de passe

- Utilisez un **mot de passe différent** pour chaque compte
- **Changez régulièrement vos mots de passe**, en particulier pour les informations les plus sensibles (banque en ligne, compte professionnel)
- Votre mot de passe doit être **long et complexe** :
  - **Au moins douze caractères**
  - Une combinaison de **lettres** majuscules et minuscules, **chiffres** et **symboles**

L%nG&K@mPl3X

  - Utilisez une phrase pour composer votre mot de passe
- Votre mot de passe **ne doit pas pouvoir être retrouvé simplement** :

  - Il ne contient pas d'information en rapport avec vous-même, votre famille ou vos amis (date de naissance, ville de résidence, prénoms…)
  - Modifiez immédiatement les mots de passe temporaires reçus par courrier électronique et supprimez ces messages
- **Stockez vos mots de passe en sécurité** :



  - Dans un calepin, rangé à distance de votre ordinateur
  - Ou dans un logiciel de gestion de mots de passe de confiance, comme ceux qui vous sont recommandés par la CNIL (voir plus bas). Pensez à réaliser une sauvegarde régulière de votre base de mots de passe.

L'authentification par double facteur

Votre banque et de plus en plus souvent vos services en ligne vous permettent d'utiliser un second facteur pour valider votre authentification. Il s'agit par exemple de fournir un code à usage unique affiché sur votre téléphone mobile ou un dispositif portable (appelé jeton ou token), d'insérer une clé USB sécurisée dans votre ordinateur, ou encore de réaliser une opération avec votre téléphone (la lecture d'un code-barres 2D), etc.

Informez-vous sur l'existence de méthodes de double authentification :

- Quand elles existent, adoptez-les (notamment pour votre courrier électronique en ligne et vos réseaux sociaux) ;
- Quand vous les utilisez, prenez l'habitude d'emporter avec vous vos moyens de seconde authentification, la sécurité ne doit pas être une gêne.

Quelques exemples de services qui proposent un double facteur d'authentification :

- Courrier électronique : Gmail (Google), iCloud, Outlook, Yahoo, …
- Réseaux sociaux : Twitter, Facebook, Google+, LinkedIn, …
- Développement Web : Drupal, Wordpress, Github, Launchpad, …

Concevoir un mot de passe complexe, mais facile à retenir

Plusieurs astuces vous sont données sur le site de la CNIL ou de l'ANSSI évoqués plus bas pour construire un mot de passe à la fois complexe et facile à retenir par vous-même. Ce type de mot de passe vous sera très utile pour les services que vous utilisez souvent ou pour la protection de la base de données de votre logiciel de gestion de mot de passe.

- Fabriquez le mot de passe à partir d'une phrase dont vous vous rappellerez facilement (une ligne de poésie, une devise, une parole de chanson) et par exemple substituez chaque mot par sa première lettre ou par un son approchant
- Alternez majuscules et minuscules ;
- Substituez les lettres par des symboles ou des chiffres ressemblants visuellement ou phonétiquement ;
- **Ou trouvez votre propre astuce qui vous est personnelle, le résultat devant être long et complexe.**

Pour aller plus loin

Nous vous proposons d'autres ressources qui contiennent des conseils complémentaires sur la sécurité du mot de passe :

- CNIL, « Construire un mot de passe sûr et gérer la liste de ses codes d'accès », https://www.cnil.fr/fr/construire-un-mot-de-passe-sur-et-gerer-la-liste-de-ses-codes-dacces
- ANSSI, « Sécurité des mots de passe » (notamment dans un contexte professionnel), http://www.ssi.gouv.fr/guide/mot-de-passe/

Exemples (pour des mots de passe complexes qu'on devra retenir) :

« Tout ce qui est mort comme fait, est vivant comme enseignement. » (Victor Hugo, Notre-Dame de Paris)

Peut donner : TcKi3Mcf;EVc€

« Il y a deux sortes de temps : y a le temps qui attend et le temps qui espère. » (Jacques Brel, L'Ostendaise)

Vous inspirera un mot de passe plus long comme : iy@2sDt:YaLTkiA&LtKi€

A vous de trouver votre méthode et vos phrases.

Pour les mots de passe que vous n'avez pas besoin de retenir parce que gérés par votre logiciel de mot de passe, laissez celui-ci calculer automatiquement des mots de passe complexes de 12 caractères au moins avec minuscules, majuscules, chiffres et symboles.