LE SAVIEZ-VOUS ?

Pour des mots de passe forts et faciles à mémoriser, j'opte pour **des phrases de passe**, comme « Pourvu qu'il fasse beau demain ! » (177 d'entropie).

Si un fournisseur de services est piraté, il est possible que les mots de passe soient compromis. Le site suivant : **haveibeenpwned.com** permet de vérifier que des accès n'ont pas été récupérés lors d'une des attaques référencées.

SUBVENTIONNÉ PAR LA VILLE DE GENÈVE

itopie

libre, éthique, durable, locale & citoyenne

Une transition numérique vertueuse et éthique !
- La transition, ça prend du temps.
- Il ne faut pas brûler les étapes.
- C'est très enrichissant et la démarche a du sens.

Venez vous faire aider chez itopie !
itopie.ch

Sources et infos sur itopie.ch/brochures

GÉRER MES MOTS DE PASSE

J'utilise des mots de passe différents et robustes, et pour cela je me fais aider par un coffre-fort à mots de passe.

LES AVANTAGES

- **Le coffre à mots de passe s'installe sur mon ordinateur ou mon téléphone.**
- **Il me permet de stocker et d'organiser mes mots de passe dans un ou plusieurs fichiers.**
- **Un générateur de mot de passe aléatoire est intégré pour créer un mot de passe en trois clics.**
- **Il gère la double authentification par TOTP*.**
- **Il peut remplir automatiquement les formulaires de connexion sur internet, sans que j'aie à taper quoi que ce soit, ce qui me simplifie la vie et accélère l'accès à mes services.**

COMMENT FAIRE ?

1. J'installe un **gestionnaire de mots de passe** et prends l'habitude de l'utiliser.
2. Je crée un nouveau fichier pour mon coffre et je définis un mot de passe principal (la clef). **C'est le seul que je dois mémoriser**.
3. Je crée **une entrée par compte**, par service en ligne, par application, chacune ayant son propre mot de passe unique et robuste.
4. J'utilise le **générateur de mot de passe** intégré, le règle pour créer un mot de passe ayant une **entropie*** de 80 au minimum, soit 12 à 14 caractères alphanumériques et spéciaux.

*LE TOTP, C'EST QUOI ?

Time based One Time Password : C'est une méthode qui utilise l'heure actuelle et un « secret » partagé pour générer un mot de passe à usage unique basé sur le temps, qui change toutes les 30 secondes.
Le TOTP est plus pratique et sécurisé que la seconde authentification par SMS ou par courriel.

*L'ENTROPIE, C'EST QUOI ?

L'entropie est le degré de hasard ou de complexité : plus ce nombre est élevé, plus les mots de passe sont forts.

Comment démarrer ma transition numérique éthique ?

SÉCURITÉ

environnement · éthique · santé

PROTÉGER LA SÉCURITÉ DE MES COMPTES

Quand je transmets des identifiants ou des informations confidentielles, je ne les envoie pas par courriel, mais j'utilise des outils en ligne pour sécuriser mon envoi.

LES AVANTAGES

- **Ne pas envoyer mes mots de passe par courriel contribue à me protéger du piratage.**

COMMENT FAIRE ?

1. Je me rends sur un service en ligne dédié à l'envoi chiffré d'informations et je renseigne les informations à transmettre dans le formulaire.
2. J'envoie le formulaire, ce qui génère un lien unique et impossible à deviner. Je communique ce lien au destinataire.
3. Exemples de service d'envoi chiffré d'informations :
   bin.inubo.ch
   kpaste.infomaniak.com

Il en existe d'autres ! Avant de les utiliser, je vérifie la politique de confidentialité du fournisseur, notamment s'il garantit que l'information secrète ne lui est pas accessible.

SÛR

COMMENT FONCTIONNENT CES OUTILS ?

- Ils chiffrent les données envoyées et les déchiffrent au moment de les afficher au destinataire.
- Le destinataire doit disposer du lien exact, qui est nécessaire pour accéder à l'information confidentielle.

Il est possible d'ajouter de la sécurité :

- Mot de passe pour accéder à l'information confidentielle (que je communique par un autre moyen)
- Effacement automatique après une utilisation
- Suppression automatique après une semaine

LE SAVIEZ-VOUS ?

Le **hameçonnage** (ou *phishing*) est une technique visant à récolter des informations en usurpant l'identité d'un tiers. Je transmets ainsi moi-même mes informations confidentielles.

Les cybercriminels utilisent souvent **la peur, la menace ou l'urgence** pour inciter à cliquer sur un lien. Ils peuvent aussi se faire passer pour des personnes ou entreprises que vous connaissez.

On peut aussi **chiffrer** ses courriels avec un système libre et open source (comme GNU Privacy Guard, ou GPG).

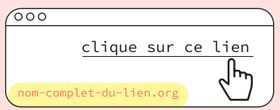
Plutôt que de transmettre un identifiant et un mot de passe, il est possible **d'inviter une personne** et lui déléguer des droits, ce qui lui permet de se connecter avec son propre compte.

PRENDRE GARDE AUX LIENS QUE JE REÇOIS

Les liens que je reçois peuvent être des tentatives pour récupérer mes accès ou d'autres informations confidentielles. Je les vérifie avant de cliquer dessus.

COMMENT FAIRE ?

- Je passe ma souris sur le lien pour vérifier que l'adresse où il mène est bien la même que le texte indiqué et qu'elle correspond bien au nom du fournisseur du service. Au survol, l'adresse est généralement indiquée en bas à gauche de la fenêtre.



- En plus de vérifier le lien sur lequel je vais cliquer, je peux contrôler l'adresse du site sur lequel je suis dans la barre d'adresse.
- Je me rends sur le site désiré en inscrivant son adresse directement dans la barre d'adresse, en général située en haut de la fenêtre (sans cliquer sur le lien).
- En cas de doute, je peux contacter le service concerné par un autre moyen (téléphone, formulaire de contact, etc.).