Certaines illustrations ont été réalisées à l'origine par Martin Vidberg pour la CNIL | https://www.cnil.fr | CC-BY-NC-ND | 2020

En cas de piratage...

- Changez le(s) mot(s) de passe compromis
- Informez les administrateurs du(des) site(s)
- Effacez les données bancaires du site
- Alertez vos amis en particulier s'il s'agit de votre adresse de courriel.
- Déconnectez à distance les terminaux liés à votre compte.
- Portez plainte

Trouvez de l'assistance sur
https://www.cybermalveillance.gouv.fr/

CYBER MALVEILLANCE .GOUV.FR

Les mots de passe sans les maux de tête

Centre de **culture numérique**
Université de Strasbourg

Mille et un comptes

Nous détenons désormais des comptes dans plusieurs sites web ou services en ligne. Nous y conservons nos précieuses données en faisant confiance au système d'identification et d'authentification.

Ce système est-il suffisant pour protéger nos données ?

Il n'y a pas de risque zéro

Comme pour toute forme de criminalité on ne peut que réduire l'essentiel des risques.
Le couple identifiant/mot de passe (identification/authentification) est soumis à des risques de vol que ce soit lors de sa création, son utilisation ou son stockage.

Mais alors que faire ?

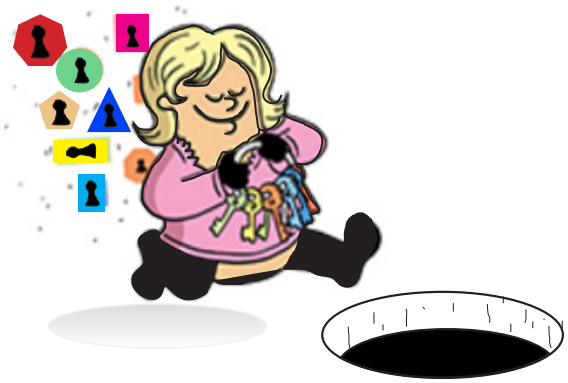
Dernières tendances

En 2022 les instances du web et de l'authentification en ligne considèrent désormais les données biométriques comme fiables (certification FIDO2*).
En particulier, avec l'appui des géants du numérique, le développement de la clé d'accès (Passkey) pourra à terme remplacer les mots de passe.

A la création d'un compte en ligne deux clés sont créées.
La première est détenue par le fournisseur du compte en ligne (clé dite publique) et la seconde ne peut être utilisée que par vous (clé privée).
Les deux clés doivent être utilisées simultanément pour accéder au compte en ligne. La clé privée se trouve, par exemple, dans votre téléphone. Elle ne répond à la clé publique que lorsque vous vous authentifiez via des données biométriques sur cet appareil.
Gardez vos mots de passe, ce n'est pas pour tout de suite...

* Fast IDentity Online Alliance est une association pour le développement et la promotion de normes d'authentification, pour l'amélioration de la sécurité et l'interoperabilité des systèmes qui les assurent.

Les pièges à éviter



- Après utilisation fermez votre session sur l'ordinateur
- Renouvellez vos mots de passe régulièrement
- Ne transmettez vos mots de passe à personne et surtout pas suite à une demande par courriel.
- Si vous vous rendez sur un site, ne cliquez pas sur un lien fourni dans un message, entrez l'adresse vous-même dans le navigateur ou utilisez vos favoris

Alerte!

Il est probable que vous ayez été piraté si, en-dehors de toute action ou demande de votre part :

- Votre mot de passe est déclaré invalide sur un site
- Un message vous parvient qui confirme le changement de votre mot de passe
- Vos contacts reçoivent des demandes d'argent depuis votre adresse
- Un site commercial confirme une commande de votre part
- Des publications de votre part apparaîssent sur un réseau social

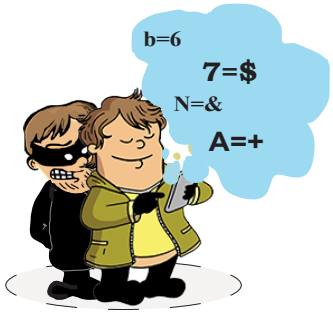
Nous pouvons décourager les attaques et nous protéger

Il est possible de dissuader le piratage en suivant quelques règles d'usage et en mettant en place des mesures qui rendent le vol de mot de passe plus difficile.
Ce fascicule, sans être exhaustif, présente les règles et techniques que tout le monde devrait connaître.

A la création d'un compte

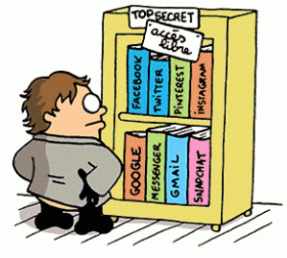
- N'utilisez jamais deux fois le même mot de passe
- Diversifiez les identifiants (par exemple en utilisant des adresses de courriel différentes)
- Créez un mot de passe complexe et long (12 caractères avec majuscules, minuscules, caractères spéciaux et chiffres)
- Créez un mot de passe qui ne soit pas fondé sur des informations connues ou accessibles de tous (mots du dictionnaire, date de naissance, nom de votre animal...)

A la connexion



- Ayez un antivirus et un pare-feu actifs pour empêcher les écoutes potentielles
- Ne vous connectez pas à un Wifi public non sécurisé
- Pour accéder à un site web, ne vous fiez pas aux liens envoyés par courriel
- Si elle est proposée par un site web, activez la double authentification*

Le stockage



- Ne conservez pas vos mots de passe en clair où que ce soit (papier, fichier, note)
- Désactivez l'option d'enregistrement des mots de passe de votre navigateur
- Ne les communiquez jamais sous quelque forme que ce soit
- Optez pour un gestionnaire de mots de passe

* Méthode par laquelle, après authentification par mot de passe, le service web fait appel à une seconde méthode d'authentification (code, biométrie ou clef) pour finaliser le processus. Depuis le 14/09/2019 les banques sont dans l'obligation de proposer une double authentification pour les paiments en ligne (sans passer par des textos).

Les gestionnaires de mots de passe

La CNIL et l'ANSSI conseillent l'utilisation d'un gestionnaire de mots de passe pour la conservation des données d'identification et d'authentification*. Ce sont des logiciels à installer sur votre navigateur ou sur vos appareils pour y stocker de manière sécurisée (chiffrée) les données de connexion ainsi que les comptes associés. Un vrai coffre-fort pour les mots de passe.

Les avantages du coffre-fort

- Un seul mot de passe est à retenir, celui du coffre-fort, pour accéder à tous les autres. (+ une double authentification).
- Vous pouvez composer des mots de passe complexes sans vous soucier de les retenir (ou demander au logiciel de les générer)
- Vous pouver y stocker d'autres données nécessaires (par exemple pour le remplissage des formulaires en ligne).

* L'Agence nationale de la sécurité des systèmes d'informations (ANSII) comme la Commission nationale de l'informatique et des libertés (CNIL) conseillent l'utilisation du logiciel libre Keepass. Il est gratuit et permet une sauvegarde locale de vos données vous protegeant ainsi du piratage potentiel d'une base de données externe.