5 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.

Depuis 2020 il existe une plateforme d'assistance :

https://www.cybermalveillance.gouv.fr/diagnostic

Derniers conseils

- Fermez votre session sur l'ordinateur que vous utilisez.
- Renouvellez vos mots de passe régulièrement
- Ne transmettez vos mots de passe à personne.
- Ne cliquez pas sur un lien transmis par courriel, tapez l'adresse ou utilisez vos favoris.

Centre de **culture numérique**
Université de Strasbourg

Mille et un comptes

Des comptes dans plusieurs sites web ou services en ligne ?
Des doutes sur le système d'identification et d'authentification.
Des craintes sur un éventuel piratage ?

Il n'y a pas de risque zéro

Le couple identifiant/mot de passe que vous utilisez peut-être dérobé de multiples façons. Comme pour toute forme de criminalité on ne peut que réduire les risques.

Mais nous pouvons décourager les attaques

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[1] présente quelques règles que tout le monde peut appliquer... et ça ne fait pas de mal à la tête.

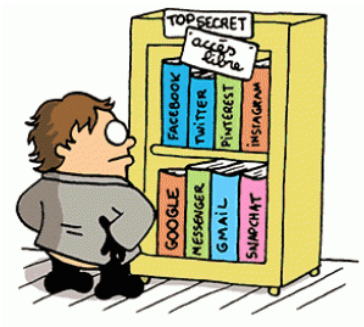
1 La création d'un compte

- 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 sans lien avec des informations connues ou accessibles de tous (mots du dictionnaire, date de naissance, nom de votre animal...)

2 La connexion

- Ayez un antivirus et un pare-feu actifs
- Ne vous connectez pas à un Wifi public non sécurisé
- Si elle est proposée par un site web, activez la double authentification[2]

3 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 communiquez jamais votre mot de passe sous quelque forme que ce soit
- Optez pour un gestionnaire de mots de passe

[2]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).

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[3]. 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.

- Un seul mot de passe est à retenir, vous pouvez composer des mots de passe complexes sans vous soucier de les retenir
- Vous pouver y stocker d'autres données nécessaires (par exemple pour le remplissage des formulaires en ligne).
- Il existe des logiciels libres et gratuits d'excellente qualité !

4 Restez 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 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

[3]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.