

Atelier Data Detox

CYBERSÉCURITÉ

Gérer ses mots de passe

❖ Utiliser un mot de passe principal avec Firefox:

Firefox peut enregistrer vos identifiants et vos mots de passe pour accéder aux services en ligne, tels que votre banque en ligne et vos comptes de courrier électronique. Si vous partagez un ordinateur avec quelqu'un, il est recommandé que vous utilisiez un mot de passe principal. **Avertissement important** : si vous n'utilisez pas de mot de passe principal sur un ordinateur publique (salle des maîtres, bibliothèques, etc.) n'importe qui ayant accès à ce même ordinateur peut voir en clair les mots de passe que vous avez enregistrés dans Firefox !

Si vous souhaitez utiliser un mot de passe principal pour protéger les identifiants et mots de passe enregistrés, consulter la marche à suivre sur le site de Firefox: [Cliquez ici](#).

❖ Gestionnaires de mots de passe : Firefox Lockwise

Firefox Lockwise synchronise les mots de passe du navigateur afin que vous puissiez les utiliser facilement pour vous connecter à vos applications Android et iOS (remplissage automatique)

- [Comment ça marche?](#)
- [Vidéo tutorielle](#)
- [Lien](#) pour le téléchargement (smartphones et ordinateurs)

❖ Autres gestionnaires de mot de passe

- [SecurSafe](#) (site suisse, gratuit jusqu'à un certain point)
- [1 password](#) (site étranger et payant)

❖ Trucs et astuces mnémotechniques :

- Choisir une phrase et y inclure des espaces, des majuscules et des caractères peu commun (@?\$#, etc.) ou choisir un refrain d'une chanson; par exemple: "Toute la musique, que j'aime" deviendrait: t5l2m7q3j6.
- Choisir l'identification à double facteurs lorsque le service le permet (En plus d'un mot de passe qui vous est demandé, vous devez renseigner votre numéro de téléphone portable par exemple, et un code d'accès au service souhaité vous est envoyé par SMS)

BIG DATA

Navigateurs

Que l'on soit sur un ordinateur ou un appareil mobile, les plus classiques sont :

- ❖ Firefox
- ❖ Safari
- ❖ Chrome

Pourquoi Firefox ?

C'est le navigateur libre et gratuit développé et distribué par Mozilla Foundation. Il s'agit d'un logiciel multi-plateforme compatible avec Windows, MAC OS X, GNU/Linux et Android. Il est le logiciel installé sur tous les ordinateurs du DIP. L'anonymat n'est pas assuré par défaut, par contre, en paramétrant Firefox, ou en ajoutant certains modules complémentaires, on peut facilement élever son niveau de confidentialité et bloquer les traqueurs.

(Sur les appareils mobiles, vous pouvez installer Firefox Klar, un navigateur dédié à la vie privée avec protection contre le pistage et blocage de contenu. Plus d'info [ici](#).)

Voici un petit exercice pour comprendre et connaître le niveau de sécurité de son navigateur (à faire sur un ordinateur ou sur un appareil mobile). Avant de débiter cette partie, n'oubliez pas de visiter [Panopticlick](#) et cliquez sur "Test Me" pour savoir si votre navigateur est unique et connaître le niveau de protection de ce dernier.

Et ensuite ?

❖ Consulter et effacer l'historique de votre navigateur

Lors de votre navigation sur Internet, de nombreuses informations sont conservées dans le navigateur, dont l'historique des pages visitées. Ces éléments peuvent être étudiés par des sites et applications tiers qui vous proposent alors un contenu personnalisé.

Comment faire ?

✓ Ordinateur

Firefox : Menu (en haut à droite) → Bibliothèque → Historique → Effacer l'historique récent

Chrome et Safari : Menu (en haut à droite) → Historique → Historique → Effacer les données de navigation

✓ Smartphone et tablette

Safari : Paramètres → Safari → Effacer historique et données de site

Firefox : Menu → Paramètres → Effacer les données privées

Chrome : Menu (en haut à droite) → Historique → Effacer les données de navigation

❖ Naviguez en "mode privé"

Utilisez cette fonctionnalité complémentaire pour réaliser des recherches sur Internet sans que les traces de navigation comme l'historique de la session ou les cookies soient enregistrés.

Comment faire ?

✓ Ordinateur

Firefox et Chrome : Menu → Nouvelle fenêtre de navigation privée

Safari : Menu → Historique → Navigation privée

✓ Smartphone et tablette

Firefox : Menu → Nouvel onglet privé

Safari : Menu → mettre en relief "privé"

Chrome : Menu → Nouvel onglet navigation privée

Booster le navigateur sur son ordinateur

Il est recommandé d'installer quelques petits modules complémentaires ou extensions à son navigateur.

Comment faire ?

✓ *Firefox et Chrome :*

- Pour bloquer les publicités et les traqueurs invisibles, installez [Privacy Badger](#).
- Pour bloquer les publicités et les traqueurs invisibles, installez [Ghostery](#).
- Pour bloquer les publicités et les traqueurs invisibles, installez [Duck Duck Go](#).
- Pour prendre conscience du pistage par des sites tiers lors de la navigation quotidienne, installez [Lightbeam](#).
- Pour s'assurer que vos connexions aux sites Internet sont dans la mesure du possible cryptées, installez [HTTPS Everywhere](#). Il s'agit d'une extension pour naviguer de manière cryptée et protégée.

Parfait ! Vous en avez fini avec le navigateur. Vous pouvez maintenant vérifier si vos actions ont porté leurs fruits: Retournez sur [Panopticlick](#) avec le navigateur que vous venez de nettoyer et cliquez sur "Test Me". Comparez les nouveaux résultats avec les précédents. Ont-ils changé ?

Moteurs de recherche

- ❖ Prendre conscience de ses activités sur Google: [directement dans votre espace Google](#)
 - Dans cet espace, il est possible d'effacer les données mémorisées par Google, soit en sélectionnant les éléments un par un, soit en les sélectionnant par groupes (sur la gauche de la page : "supprimer l'activité")
 - Télécharger ses données sur Google: Vous pouvez avoir un aperçu d'une partie des choses que Google sait de vous (et de ce qui reste enregistré sur leurs serveurs) en [téléchargeant vos données](#). Vous y retrouverez notamment :
 - Toutes vos recherches sur Google

- Les vidéos visionnées sur youtube
- Vos déplacements (si activé sur téléphone)
- ...

❖ Moteurs de recherche alternatifs

- [Duck Duck Go](#): moteur de recherche américain respectueux de la vie privée. Aucune information personnelle n'est stockée. Les résultats sont neutres et non influencés par les précédentes recherches.
 - Exercice : comparez les résultats de recherches pour un même terme sur Duck Duck Go et sur Google par exemple.
- [Qwant](#): moteur de recherche français respectueux de la vie privée. Aucune information personnelle n'est stockée. Les résultats sont neutres et non influencés par les précédentes recherches.

❖ Et encore :

- [Track This](#), pour brouiller les pistes sur votre identité personnelle en ouvrant 100 onglets en lien avec une identité qui n'est pas la vôtre... Qui n'a jamais rêvé de devenir quelqu'un d'autre?

❖ Droit à l'oubli : Il vous est possible de demander le droit à l'oubli aux différents services de référencement sur Internet. Bien que la procédure n'aboutisse que rarement, il vaut la peine de tenter le coup : [demande de droit à l'oubli sur Google](#)

Géolocalisation

❖ Consulter ses localisations :

- *iOS* : Réglages → Confidentialité → Service de localisation → Service système (tout en bas) → Lieux fréquents
- *Android* : Ouvrir Google Maps → Menu → Paramètres → Historique Maps

❖ Empêcher la géolocalisation :

- *iOS* : Réglages → Confidentialité → Service de localisation
- *Android* : Paramètres → Applications → Paramètres → Autorisation des applis → Position

❖ Désactiver la localisation :

- *iOS* : Réglages → Confidentialité → Service de localisation → Désactiver service de localisation
- *Android* : Paramètres → Localisation → Désactivé
- ❖ Supprimer les réseaux WiFi déjà enregistrés :
 - *iOS* : Réglages → Général → Réinitialiser → Réinitialiser les réglages réseaux
 - *Android* : Paramètres → WiFi → Menu → Réseaux enregistrés
- ❖ Changer le nom du téléphone pour ne pas être repéré comme : "Natel de Stéphane Bertrand"
 - *iOS* : Réglages → Général → Informations → Clique sur la première ligne, qui contient le nom de ton appareil. Renomme ton appareil, puis clique sur Terminé.
 - *Android* : Paramètres → A propos du téléphone → Nom de l'appareil

RÉSEAUX SOCIAUX

Facebook

- ❖ Pour prendre conscience de ce que Facebook sait de moi :

Depuis la version ordinateur de Facebook : Clique en haut à droite sur la petite flèche qui pointe en bas → Paramètres → Vos informations Facebook → Télécharger vos informations → Créer un fichier

- ❖ Pour modifier les paramètres de confidentialité sur Facebook :

Depuis la version ordinateur de Facebook : Clique en haut à droite sur la petite flèche qui pointe en bas → Paramètres → Confidentialité → Télécharger vos informations → Créer un fichier

- ❖ Pour prendre conscience de comment Facebook cible ses publicités en fonction de ce qu'ils savent de moi :

Depuis la version ordinateur de Facebook : Clique en haut à droite sur la petite flèche qui pointe en bas → Paramètres → Publicités → Vos centres d'intérêt / Vos informations

CYBERHARCÈLEMENT

Il existe plusieurs dépliants très utiles sur les questions liées au cyberharcèlement :

- ❖ [A l'attention des élèves](#)
- ❖ [A l'attention des parents](#)
- ❖ [A l'attention des professionnels](#)